日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

13.09.00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　８月２７日

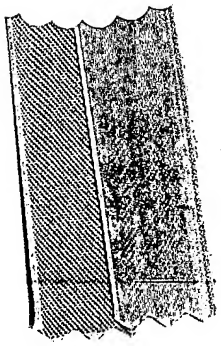
出願番号
Application Number: 平成１１年特許願第２４１７４７号

出願人
Applicant (s): 富士通株式会社
株式会社日立製作所
日本コロムビア株式会社
三洋電機株式会社

JP00/05770

4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



２０００年１０月２０日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８５３１８

【書類名】　特許願

【整理番号】　1990901

【提出日】　平成11年 8月27日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 11/08

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畑中　正行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　蒲田　順

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畠山　卓久

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　東京都小平市上水本町５丁目２０番１号　株式会社日立製作所　半導体グループ内

【氏名】　木下　泰三

【発明者】
【住所又は居所】　東京都港区赤坂四丁目１４番１４号　日本コロムビア株式会社内
【氏名】　穴澤　健明
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　日置　敏昭
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　金森　美和
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　堀　吉宏
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【特許出願人】
【識別番号】　000005108
【住所又は居所】　東京都千代田区神田駿河台４丁目６番地
【氏名又は名称】　株式会社日立製作所
【特許出願人】
【識別番号】　000004167
【住所又は居所】　東京都港区赤坂四丁目１４番１４号
【氏名又は名称】　日本コロムビア株式会社

【特許出願人】

【識別番号】　000001889

【住所又は居所】　大阪府守口市京阪本通２丁目５番５号

【氏名又は名称】　三洋電機株式会社

【代理人】

【識別番号】　100064746

【弁理士】

【氏名又は名称】　深見　久郎

【選任した代理人】

【識別番号】　100085132

【弁理士】

【氏名又は名称】　森田　俊雄

【選任した代理人】

【識別番号】　100091409

【弁理士】

【氏名又は名称】　伊藤　英彦

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ配信システム

【特許請求の範囲】

【請求項１】　コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第１のインターフェース部と

前記暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記第１のインターフェース部に与えるためのセッションキー暗号化部と、

前記第１の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのコンテンツキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第１のライセンスデータ暗号処理部と、

前記第１のライセンスデータ暗号処理部の出力を第２の共通鍵でさらに暗号化して前記第１のインターフェース部に与え配信するための第２のライセンスデータ暗号処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第２のインターフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部と、

前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部と、

第２の公開暗号化鍵を保持するための第２の鍵保持部と、

前記第２の公開暗号化鍵を、前記第１の共通鍵に基づいて暗号化し、前記第２のインターフェース部に出力するための第１の暗号化処理部と、

前記第２のライセンスデータ暗号処理部からの暗号化されたコンテンツキーを受け、前記第２の共通鍵に基づいて復号化するための第２の復号処理部と、

前記第２の復号処理部の出力を受けて、格納するための第１の記憶部と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部と、

前記第１の記憶部に格納されたデータに基づいて、前記第２の秘密復号鍵により前記コンテンツキーを復号するための第３の復号処理部とを備える、データ配信システム。

【請求項２】　前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第１の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第２の秘密復号鍵は、前記メモリカードごとに異なる、請求項１記載のデータ配信システム。

【請求項３】　前記第２および第３の復号処理部は、前記コンテンツデータ供給装置において前記第２の公開暗号化鍵で暗号化され、さらに前記第２の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを前記第２のインターフェース部を介して受け、前記第２の共通鍵および前記第２の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第２の記憶部をさらに備える、請求項２記載のデータ配信システム。

【請求項４】　前記第１の共通鍵と前記第２の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第１のセッションキー発生部により生成された同一の鍵データである、請求項３記載のデータ配信システム。

【請求項５】　前記第１の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格

納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第３の復号処理部からの前記コンテンツキーを受けて、第３の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第３の共通鍵を生成する第２のセッションキー発生部と、

前記配信データ解読部からの前記第３の共通鍵により暗号化された前記コンテンツキーを受けて復号して抽出し、前記第１の記憶部から出力された前記暗号化コンテンツデータを前記コンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項４記載のデータ配信システム。

【請求項６】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、

前記第２の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第３の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第３の公開暗号化鍵を復号して抽出し、

前記第２の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記コンテンツキーおよび前記ライセンス情報データを前記第３の公開暗号化鍵で暗号化し、

前記第１の暗号化処理部は、前記第２の暗号化処理部の出力を受けて、前記第３の共通鍵に基づいて暗号化して前記第２のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第２の記憶部に格納されている前記ライセンス情報データを消去し、

前記第１の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項５記載のデータ配信システム。

【請求項７】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第１の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項５記載のデータ配信システム。

【請求項８】　前記配信データ解読部は、

前記第２の共通鍵を生成するための第３のセッションキー発生部と、

前記第３のセッションキー発生部の出力を暗号化して前記第２のインターフェース部に与えることが可能な第３の暗号化処理部とをさらに含む、請求項３記載のデータ配信システム。

【請求項９】　前記第１の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第３の暗号処理部は、第４の公開暗号化鍵により前記第３のセッションキー発生部の出力を暗号化して前記第２のインターフェース部に与え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第３の復号処理部からの前記コンテンツキーを受けて、第３の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第３の共通鍵を生成する第２のセッションキー発生部と、

前記第４の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部と、

前記第４の公開暗号化鍵で暗号化された前記第２の共通鍵を復号可能な公開鍵復号部と、

前記配信データ解読部からの前記第３の共通鍵により暗号化された前記コンテンツキーを受けて復号して抽出し、前記第１の記憶部から出力された前記暗号化コンテンツデータを前記コンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項８記載のデータ配信システム。

【請求項１０】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、

前記第２の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第３の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第３の公開暗号化鍵を復号して抽出し、

前記第２の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記コンテンツキーおよび前記ライセンス情報データを前記第３の公開暗号化鍵で暗号化し、

前記第１の暗号化処理部は、前記第２の暗号化処理部の出力を受けて、前記第３の共通鍵に基づいて暗号化して前記第２のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第２の記憶

部に格納されている前記ライセンス情報データを消去し、

前記第１の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項９記載のデータ配信システム。

【請求項１１】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第１の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項９記載のデータ配信システム。

【請求項１２】　前記第１のインターフェース部と前記第２のインターフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

前記第１の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項１記載のデータ配信システム。

【請求項１３】　前記第１のインターフェース部は、

前記端末と直接接続可能なコネクタ部を含む、請求項１記載のデータ配信システム。

【請求項１４】　前記第１のインターフェース部は、

前記メモリーカードと直接接続可能な接続部を含む、請求項２記載のデータ配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

【０００２】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【０００４】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽情報のコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行う個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【０００７】

しかも、ＣＤからＭＤへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、１つのＭ

Ｄからさらに他のＭＤに音楽情報をデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

【０００８】

すなわち、現状においては、デジタル記録媒体であるＣＤからＭＤへのコピーは、親から子へのコピーは自由に行なうことができるものの、孫へのコピーを行なうことはできない。

【０００９】

【発明が解決しようとする課題】

そのような事情からも、音楽情報や画像情報をデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【００１０】

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権原のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権原を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

【００１１】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

【００１２】

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

【００１３】

【課題を解決するための手段】

請求項１記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するため

の第１のインターフェース部と暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部と、ユーザの端末に対応して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化して第１のインターフェース部に与えるためのセッションキー暗号化部と、第１の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、暗号化コンテンツデータを復号するためのコンテンツキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化するための第１のライセンスデータ暗号処理部と、第１のライセンスデータ暗号処理部の出力を第２の共通鍵でさらに暗号化して第１のインターフェース部に与え配信するための第２のライセンスデータ暗号処理部とを備え、各端末は、外部との間でデータを授受するための第２のインターフェース部と、暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、配信データ解読部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部と、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理するための第１の復号処理部と、第２の公開暗号化鍵を保持するための第２の鍵保持部と、第２の公開暗号化鍵を、第１の共通鍵に基づいて暗号化し、第２のインターフェース部に出力するための第１の暗号化処理部と、第２のライセンスデータ暗号処理部からの暗号化されたコンテンツキーを受け、第２の共通鍵に基づいて復号化するための第２の復号処理部と、第２の復号処理部の出力を受けて、格納するための第１の記憶部と、第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部と、第１の記憶部に格納されたデータに基づいて、第２の秘密復号鍵によりコンテンツキーを復号するための第３の復号処理部とを備える。

【００１４】

請求項２記載のデータ配信システムは、請求項１記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第１の公開暗号化鍵は、メモリカードの種類に対応して予め定められた鍵であり、第２の公開暗号化鍵は、メモリカードごとに異なる。

【００１５】

請求項３記載のデータ配信システムは、請求項２記載のデータ配信システムの構成に加えて、第２および第３の復号処理部は、コンテンツデータ供給装置において第２の公開暗号化鍵で暗号化され、さらに第２の共通鍵で暗号化されて、コンテンツキーとともに配信されるライセンス情報データを第２のインターフェース部を介して受け、第２の共通鍵および第２の秘密復号鍵に基づいて復号し、配信データ解読部は、復号されたライセンス情報データを格納する第２の記憶部をさらに備える。

【００１６】

請求項４記載のデータ配信システムは、請求項３記載のデータ配信システムの構成に加えて、第１の共通鍵と第２の共通鍵とは、暗号化コンテンツデータの通信の際に、第１のセッションキー発生部により生成された同一の鍵データである。

【００１７】

請求項５記載のデータ配信システムは、請求項４記載のデータ配信システムの構成に加えて、第１の記憶部は、コンテンツキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第１の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第３の復号処理部からのコンテンツキーを受けて、第３の共通鍵に基づいて暗号化して出力し、第１の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第３の共通鍵を生成する第２のセッションキー発生部と、配信データ解読部からの第３の共通鍵により暗号化されたコンテンツキーを受けて復号して抽出し、第１の記憶部から出力された暗号化コンテンツデータをコンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【００１８】

請求項６記載のデータ配信システムは、請求項５記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、第２の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第３の共通鍵に基づいて暗号化されて他の端末の側から送信される第３の公開暗号化鍵を復号して抽出し、第２の暗号化処理部は、移動動作モードが指定されるのに応じて、コンテンツキーおよびライセンス情報データを第３の公開暗号化鍵で暗号化し、第１の暗号化処理部は、第２の暗号化処理部の出力を受けて、第３の共通鍵に基づいて暗号化して第２のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第２の記憶部に格納されているライセンス情報データを消去し、第１の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００１９】

請求項７記載のデータ配信システムは、請求項５記載のデータ配信システムの構成に加えて、記配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第１の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００２０】

請求項８記載のデータ配信システムは、請求項３記載のデータ配信システムの構成に加えて、配信データ解読部は、第２の共通鍵を生成するための第３のセッションキー発生部と、第３のセッションキー発生部の出力を暗号化して第２のインターフェース部に与えることが可能な第３の暗号化処理部とをさらに含む。

【００２１】

請求項９記載のデータ配信システムは、請求項８記載のデータ配信システムの構成に加えて、第１の記憶部は、コンテンツキーに基づいて復号できる暗号化コ

ンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第３の暗号処理部は、第４の公開暗号化鍵により第３のセッションキー発生部の出力を暗号化して第２のインターフェース部に与え、第１の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第３の復号処理部からのコンテンツキーを受けて、第３の共通鍵に基づいて暗号化して出力し、第１の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第３の共通鍵を生成する第２のセッションキー発生部と、第４の公開暗号化鍵を配信データ解読部に与える公開鍵保持部と、第４の公開暗号化鍵で暗号化された第２の共通鍵を復号可能な公開鍵復号部と、配信データ解読部からの第３の共通鍵により暗号化されたコンテンツキーを受けて復号して抽出し、第１の記憶部から出力された暗号化コンテンツデータをコンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【００２２】

請求項１０記載のデータ配信システムは、請求項９記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、第２の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第３の共通鍵に基づいて暗号化されて他の端末の側から送信される第３の公開暗号化鍵を復号して抽出し、第２の暗号化処理部は、移動動作モードが指定されるのに応じて、コンテンツキーおよびライセンス情報データを第３の公開暗号化鍵で暗号化し、第１の暗号化処理部は、第２の暗号化処理部の出力を受けて、第３の共通鍵に基づいて暗号化して第２のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第２の記憶部に格納されているライセンス情

報データを消去し、第１の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００２３】

請求項１１記載のデータ配信システムは、請求項９記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第１の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００２４】

請求項１２記載のデータ配信システムは、請求項１記載のデータ配信システムの構成に加えて、第１のインターフェース部と第２のインターフェース部とは、携帯電話網により接続され、コンテンツデータ供給装置は、

第１の公開暗号鍵に基づいて、ユーザの認証を行なう。

【００２５】

請求項１３記載のデータ配信システムは、請求項１記載のデータ配信システムの構成に加えて、第１のインターフェース部は、端末と直接接続可能なコネクタ部を含む。

【００２６】

請求項１４記載のデータ配信システムは、請求項２記載のデータ配信システムの構成に加えて、第１のインターフェース部は、メモリーカードと直接接続可能な接続部を含む。

【００２７】

【発明の実施の形態】

［実施の形態１］

［システムの全体構成］

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【００２８】

なお、以下では携帯電話網を介して、デジタル音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物情報データ、たとえば画像情報等の著作物情報データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

【００２９】

図１を参照して、著作権の存在する音楽情報を管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリアである携帯電話会社２０に、このような暗号化データを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきたユーザが正規のユーザであるか否かの認証を行う。

【００３０】

携帯電話会社２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。配信サーバ１０は、配線リクエストがあると、認証サーバ１２によりユーザが正規のユーザであることを確認し、要求された音楽情報をさらに暗号化したうえで、携帯電話会社２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【００３１】

図１においては、たとえば携帯電話ユーザ１の携帯電話１００には、携帯電話１００により受信された暗号化された音楽データを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話１００中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード１１０が装着される構成となっている。

【００３２】

さらに、たとえばユーザ１は、携帯電話１００に接続したヘッドホン１３０等を介してこのような再生された音楽データを聴取することが可能である。

【００３３】

以下では、このような配信サーバ１０と認証サーバ１２と配信キャリア（携帯電話会社）２０とを併せて、音楽サーバ３０と総称することにする。

【００３４】

また、このような音楽サーバ３０から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【００３５】

このような構成とすることで、まず、メモリカード１１０を購入していない正規のユーザでないものは、音楽サーバ３０からの配信データを受取って再生することが困難な構成となる。

【００３６】

しかも、配信キャリア２０において、たとえば１曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００３７】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【００３８】

このとき、たとえばメモリカード１１２を有するユーザ２が、自己の携帯電話１０２により、音楽サーバ３０から直接音楽データの配信を受けることは可能である。しかしながら、相当量の情報量を有する音楽データ等をユーザ２が直接音楽サーバ３０から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該音楽データの配信を受けているユーザ１から、その音楽情報をコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

【００３９】

しかしながら、著作権者の権利保護の観点からは、自由な音楽データのコピーを放任することはシステム構成上許されない。

【００４０】

図１に示した例では、ユーザ１が受信した音楽データを、デジタル音楽データそのものおよび当該音楽データを再生可能とするために必要な情報とともに、ユーザ２に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合、ユーザ１は、再生のために必要な情報（再生情報）ごとユーザ２にコピーさせるため、情報の移動を行なった後には、ユーザ１においては音楽データの再生を行なうことは不可能とする必要がある。ここで、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化されたコンテンツデータを復号可能なコンテンツキー（「ライセンスキー」とも称する）と、著作権保護に関わる情報であるライセンスＩＤデータやユーザＩＤデータ等のライセンス情報とを意味する。

【００４１】

これに対して、音楽データ（コンテンツデータ）のみを暗号化されたままの状態で、ユーザ２にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【００４２】

この場合、ユーザ２の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないので、ユーザ２は、コンテンツデータを得ただけでは、音楽情報を再生させることができない。したがって、ユーザ２が、このような音楽情報の再生を望む場合は、改めて音楽サーバ３０からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいため、ユーザ２が直接音楽サーバ３０からすべての情報の配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【００４３】

たとえば、携帯電話１００および１０２が、ＰＨＳ（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１からユーザ２への一括した情報の移転（移動）や、コンテンツデータのみの転送（複製）を行なうことが可能である。

【００４４】

図１に示したような構成においては、暗号化して配信される音楽データ（コン

テンツデータ）をユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第２には、配信データを暗号化する方式そのものであり、さらに、第３には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

【００４５】

［暗号／復号キーの構成］

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【００４６】

まず、図１に示した構成において、メモリカード１００内のデータ処理を管理するための鍵としては、メモリカードという媒体の種類に固有であり、かつ、メモリカードの種類等を個別に特定するための情報を含む秘密復号鍵Ｋｍｅｄｉａ（ｎ）（ｎ：自然数）と、メモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）と、公開暗号化鍵ＫＰｃａｒｄ（ｎ）により暗号化されたデータを復号するための秘密復号鍵Ｋｃａｒｄ（ｎ）とがある。

【００４７】

ここで、鍵Ｋｃａｒｄ（ｎ）や鍵ＫＰｃａｒｄ（ｎ）の表記中の自然数ｎは、各メモリカードを区別するための番号を表わす。

【００４８】

すなわち、公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されたデータは、各メモリカードごとに存在する秘密復号鍵Ｋｃａｒｄ（ｎ）で復号可能である。したがって、メモリカードにおける配信データの授受にあたっては、基本的には、後に説明するように３つの暗号鍵Ｋｍｅｄｉａ（ｎ）、Ｋｃａｒｄ（ｎ）、ＫＰｃａｒｄ（ｎ）が用いられることになる。

【００４９】

さらに、メモリカード外とメモリカード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）と、公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）により暗号化されたデータを復号化するた

めの秘密復号鍵Ｋｍｅｄｉａ（ｎ）と、各通信ごと、たとえば、サーバ３０へのユーザのアクセスごとにサーバ３０、携帯電話機１００または１０２において生成される共通鍵Ｋｓが用いられる。

【００５０】

ここで、共通鍵Ｋｓは、たとえば、ユーザが音楽サーバ３０に対して１回のアクセスを行なうごとに発生する構成として、１回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

【００５１】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ｋｓを「セッションキー」とも呼ぶことにする。

【００５２】

したがって、共通鍵Ｋｓは各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

【００５３】

また、配信されるべきデータについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるＫｃ（以下、ライセンスキーと呼ぶ）があり、この共通鍵Ｋｃにより暗号化されたコンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等が存在する。一方、携帯電話は、受信者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤを保持している。

【００５４】

このような構成とすることで、ライセンスＩＤデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザＩＤデータを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

【００５５】

配信データにおけるコンテンツデータＤｃは、上述のとおり、たとえば音楽情報データであり、このコンテンツデータをライセンスキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

【００５６】

ここで、［Ｙ］Ｘという表記は、データＹを、鍵データＸにより復号可能な暗号に変換した情報であることを示している。

【００５７】

［音楽サーバ３０の構成］

図３は、図１に示した音楽サーバ３０の構成を示す概略ブロック図である。音楽サーバ３０は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００５８】

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、公開暗号化鍵ＫＰｍｅｄｉａにより暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話においてセッションキーＫｓにより暗号化されたうえで送信されたデータを通信装置３５０およびデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンスキーやライセンスＩＤ等のデータを配信制御部３１２に制御されて暗号化するための暗号化処理部３２

０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１を介して通信装置３５０に与える暗号化処理部３２２とを含む。

【００５９】

［端末（携帯電話機）の構成］

図４は、図１に示した携帯電話１００の構成を説明するための概略ブロック図である。

【００６０】

携帯電話１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話１００の動作を制御するためのコントローラ１１０６と、受信者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤを保持するユーザＩＤ保持部１１０７と、外部からの指示を携帯電話１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスＢＳ２に与え得る信号に変換し、または、データバスＢＳ２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インターフェース部１１２２とを備える。

【００６１】

ここで、ユーザＩＤデータは、たとえばユーザの電話番号等のデータを含む。

携帯電話１００は、さらに、サーバ３０からの音楽データを復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００と、メモリカード１１０と携帯電話の他の部分とのデータ授受にあたり、データバスＢＳ

２上においてやり取りされるデータを暗号化するためのセッションキーＫｓを乱数等により発生するセッションキー発生部１５０２と、セッションキー発生部１５０２により生成されたセッションキーを暗号化して、データバスＢＳ２に与えるための暗号化処理部１５０４と、セッションキー発生部１５０２において生成された、データバスＢＳ２上のデータをセッションキーＫｓにより復号して出力する復号処理部１５０６と、復号処理部１５０６の出力を受けて、音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２と、デジタルアナログ変換部１５１２の出力を受けて、ヘッドホン１３０と接続するための接続端子１５１４とを含む。

【００６２】

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、形態電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【００６３】

［メモリカードの構成］

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【００６４】

以下では、端末１００に装着されるメモリカード１１０の公開暗号化キーＫＰｍｅｄｉａと、端末１０２に装着されるメモリカード１１２の公開暗号化キーＫＰmediaとを区別して、それぞれ、メモリカード１１０に対するものを公開暗号化キーＫＰｍｅｄｉａ（１）と、メモリカード１１２に対するものを公開暗号化キーＫＰmedia（２）と称することにする。

【００６５】

また、これに対応して、公開暗号化キーＫＰｍｅｄｉａ（１）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーＫｍ

ｅｄｉａ（１）と称し、公開暗号化キーＫＰｍｅｄｉａ（２）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーＫｍｅｄｉａ（２）と称することにする。

【００６６】

このように、媒体固有の公開暗号化キーを区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

【００６７】

メモリカード１１０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、公開暗号化キーＫＰｍｅｄｉａ（１）の値を保持し、データバスＢＳ３に公開暗号化キーＫＰｍｅｄｉａ（１）を出力するためのＫＰｍｅｄｉａ（１）保持部１４０１と、カード１１０に対応する秘密復号鍵Ｋｍｅｄｉａ（１）を保持するためのＫｍｅｄｉａ（１）保持部１４０２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理をすることにより、セッションキーＫｓを抽出する復号処理部１４０４と、公開暗号化キーＫＰｃａｒｄ（１）を保持するためのＫＰｃａｒｄ（１）保持部１４０５と、復号処理部１４０４により抽出されたセッションキーＫｓに基づいて、切換スイッチ１４０８からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４０６と、データバスＢＳ３上のデータを復号処理部１４０４により抽出されたセッションキーＫｓにより復号処理してデータバスＢＳ４に与えるための復号処理部１４１０と、データバスＢＳ４からメモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されているライセンスキーＫｃ、ライセンスＩＤ等のデータを格納し、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納するためのメモリ１４１２とを備える。

【００６８】

切換えスイッチ１４０８は、接点Ｐａ、Ｐｂ、Ｐｃを有し、接点ＰａにはＫＰ

ｃａｒｄ（１）保持部１４０５からの公開暗号化キーＫＰｃａｒｄ（１）が，接点ＰｂにはデータバスＢＳ５が、接点Ｐｃには暗号化処理部１４１４の出力が与えられる。切換えスイッチ１４０８は、それぞれ、接点Ｐａ、Ｐｂ、Ｐｃに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部１４０６に与える。

【００６９】

メモリカード１１０は、さらに、キーＫｃａｒｄ（１）の値を保持するためのＫｃａｒｄ（１）保持部１４１５と、公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化されており、かつ、メモリ１４１２から読出されたライセンスキーＫｃ、ライセンスＩＤ等（［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１））を、復号処理してデータバスＢＳ５に与える復号処理部１４１６と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵ＫＰｃａｒｄ（ｎ）を復号処理部１４１０から受けて、この相手方の公開暗号化鍵ＫＰｃａｒｄ（ｎ）に基づいて、データバスＢＳ５上に出力されているライセンスキーＫｃ、ライセンスＩＤ等を暗号化したうえで、切換スイッチ１４０８に出力するための暗号化処理部１４１４と、データバスＢＳ３を介して外部とデータの授受を行い、データバスＢＳ５との間でライセンスＩＤデータ等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０と、データバスＢＳ５との間でライセンスＩＤデータ等のデータの授受が可能なレジスタ１５００とを備える。

【００７０】

なお、図５において実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。

【００７１】

このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

【００７２】

もちろん、メモリ１４１２も含めて、モジュールＴＲＭ内に組み込まれる構成

としてもよい。しかしながら、図５に示したような構成とすることで、メモリ１４１２中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１２中のデータのみでは、音楽データを再生することは不可能であり、かつ高価なタンブルレジスタンスモジュール内にメモリ１４１２を設ける必要がないので、製造コストが低減されるという利点がある。

【００７３】

図６および図７は、図１および図３～図５で説明したデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【００７４】

図６および図７においては、ユーザ１が、メモリカード１１０を用いることで、音楽サーバ３０から音楽データの配信を受ける場合の動作を説明している。

【００７５】

まず、ユーザ１の携帯電話機１００から、ユーザによりキーボード１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【００７６】

カード１１０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化キーＫＰｍｅｄｉａ（１）をサーバ３０に対して送信する（ステップＳ１０２）。

【００７７】

サーバ３０では、カード１１０から転送された配信リクエストならびにキーＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０４）、受信したキーＫＰｍｅｄｉａ（１）に基づいて、認証サーバ１２に対して照会を行ない、正規ユーザからのアクセスの場合は次の処理に移行し（ステップＳ１０６）、正規ユーザでない場合には、処理を終了する（ステップＳ１５４）。

【００７８】

照会の結果、正規ユーザであることが確認されると、サーバ３０では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、サーバ３０内の暗号化処理部３１６が、受信したキーＫＰｍｅｄｉａ（１）により、このセ

ッションキーＫｓを暗号化してデータ［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

【００７９】

続いて、サーバ３０は、データ［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化データ［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１００のメモリカード１１０に対して送信する（ステップＳ１１０）。

【００８０】

携帯電話機１００が、データ［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、キーデータＫｍｅｄｉａ（１）により復号処理することにより、セッションキーデータＫｓを復号し抽出する（ステップＳ１１４）。

【００８１】

続いて、配信動作においては、切換スイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１１０に対する公開暗号化鍵）を、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ１１８）。

【００８２】

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓをサーバ３０に対して送信する（ステップＳ１２０）。

【００８３】

サーバ３０では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、キーデータＫＰｃａｒｄ（１）を復号抽出する（ステップＳ１２４）。

【００８４】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

【００８５】

さらに、サーバ３０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１１０に送信する（ステップＳ１２８）。

【００８６】

携帯電話機１００がデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１１０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

【００８７】

一方、サーバ３０は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのキーデータＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられたキーデータＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

【００８８】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓをカード１１０に対して送信する。

【００８９】

携帯電話１００がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを受信すると（ステップＳ１４２）、カード１１０においては、復号処理部１４１０がセッションキーＫｓにより復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ１４６）。

【００９０】

さらに、カード１１０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

【００９１】

以上のような動作により、メモリカード自身が、セッションキーＫｓを送る側（サーバ３０）に、公開暗号化キーＫＰｍｅｄｉａ（１）を送信した上で、配信を受けることができ、メモリカード１１０は、音楽情報を再生可能な状態となる。以下では、メモリカードが音楽情報を再生可能な状態となっていることを、「メモリカード１１０は、状態ＳＡにある」と呼ぶことにする。一方、メモリカードが音楽情報を再生不可能な状態となっていることを、「メモリカード１１０は、状態ＳＢにある」と呼ぶことにする。

【００９２】

さらに、メモリカード１１０からサーバ３０へは、配信受理が通知され、サーバ３０で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

【００９３】

図８は、携帯電話１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【００９４】

図８を参照して、携帯電話のキーボード１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１１０に対して出力される（ステップＳ２００）。

【００９５】

カード１１０においては、この再生リクエストに応じて、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データに基づいて、復号可

能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、復号可能と判断した場合は、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話１００に対して送信する（ステップＳ２０４）。一方、復号不可能と判断した場合は、処理を終了する（ステップＳ２３０）。

【００９６】

復号可能と判断され、カード１１０から公開暗号化キーＫＰｍｅｄｉａ（１）が送信された場合、携帯電話１００では、カード１１０からのキーＫＰｍｅｄｉａ（１）を受信すると（ステップＳ２０６）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成し、暗号化処理部１５０４が、キーＫＰｍｅｄｉａ（１）により、セッションキーＫｓを暗号化してデータ［Ｋｓ］ＫＰｍｅｄｉａ（１）を生成し、データバスＢＳ２を介して、カード１１０に対して送信する（ステップＳ２０８）。

【００９７】

メモリカード１１０は、データバスＢＳ２を介して、携帯電話機により生成され、かつ暗号化されたセッションキーＫｓを受け取り、キーデータＫｍｅｄｉａ（１）により復号し、セッションキーＫｓを抽出する（ステップＳ２１０）。

【００９８】

続いて、メモリカード１１０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読出し、復号処理部１４１６が復号処理を行なう（ステップＳ２１２）。

【００９９】

キーＫｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２１４）、ライセンスキーＫｃが抽出される（ステップＳ２１６）。　一方、復号不可能の場合、処理は終了する（ステップＳ２３２）。

【０１００】

メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２１４）は、レジスタ１５００内のライセンス情報データのうち、再生回数に関するデ

ータが変更される（ステップＳ２１８）。

【０１０１】

続いて、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２２０）、暗号化されたライセンスキー［Ｋｃ］Ｋｓをデータバス ＢＳ２に与える（ステップＳ２２２）。

【０１０２】

携帯電話機１００の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２４）。

【０１０３】

続いて、メモリカード１１０は、暗号化されたコンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２２６）。

【０１０４】

携帯電話機の音楽再生部１５０８は、暗号化されたコンテンツデータ［Ｄｃ］Ｋｃを、抽出されたキーデータＫｃにより復号処理して平文の音楽データを生成し（ステップＳ２２８）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ２３０）。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

【０１０５】

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化キーＫＰｍｅｄｉａ（１）を送信した上で、再生動作を行うことが可能となる。

【０１０６】

図９および図１０は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

【０１０７】

まず、携帯電話機１０２が送信側であり、携帯電話機１００が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。

【０１０８】

携帯電話機１０２は、まず、自身の側のメモリカード１１２および携帯電話１００に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

【０１０９】

カード１１２は、これに応じて、メモリ１４１２内のデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１１０に対して出力し（ステップＳ３０２）、一方、携帯電話１００は、携帯電話１０２からリクエストを受信して（ステップＳ３０１）、メモリカード１１０では、データ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

【０１１０】

続いて、携帯電話１０２および１００においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６′）、「移動リクエスト」である場合、カード１１２は、公開暗号化キーＫＰｍｅｄｉａ（２）を携帯電話機１０２に対して送信し（ステップＳ３０８）、携帯電話１０２は、キーＫＰｍｅｄｉａ（２）を受信する（ステップＳ３１２）。一方、カード１１０は、「移動リクエスト」である場合、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１００に出力し（ステップＳ３０８′）、携帯電話１００は、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１０２に対して送信する（ステップＳ３１０）。

【０１１１】

携帯電話機１０２が、キーＫＰｍｅｄｉａ（１）およびキーＫＰｍｅｄｉａ（２）を受信すると（ステップＳ３１２、ステップＳ３１２′）、携帯電話機１０２においては、セッションキー発生回路１５０２は、セッションキーＫｓを生成し（ステップＳ３０３）、公開暗号化キーＫＰｍｅｄｉａ（１）およびキーＫＰ

ｍｅｄｉａ（２）を用いて、暗号化処理部１５０４がセッションキーＫｓを暗号化する（ステップＳ３１４）。

【０１１２】

携帯電話機１０２は、データバスＢＳ２を介して、カード１１２に対しては暗号化されたセッションキー［Ｋｓ］ＫＰｍｅｄｉａ（２）を伝達し、　カード１１２においては、キーデータＫｍｅｄｉａ（２）によりセッションキーＫｓを復号抽出する（ステップＳ３２８）。

【０１１３】

さらに、携帯電話機１０２は、暗号化されたセッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信する（ステップＳ３１６）。携帯電話機１００は、データ［Ｋｓ］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、カード１１０に伝達し、カード１１０は、復号処理部１４０４が復号して、セッションキーＫｓを受理する（ステップＳ３２０）。

【０１１４】

カード１１０においては、セッションキーＫｓによりカード１１０の公開暗号化キーＫＰｃａｒｄ（１）を暗号化して（ステップＳ３２２）、携帯電話機１００から携帯電話機１０２に対して暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓを送信する（ステップＳ３２４）。携帯電話機１０２は、データ［ＫＰｃａｒｄ（１）］Ｋｓを受信し（ステップＳ３２６）、かつ、カード１１２によるキーＫｓの受理が完了すると（ステップＳ３２８）、カード１１２においては、カード１１０から送信された暗号化データ［ＫＰｃａｒｄ（１）］Ｋｓをセッションキー Ｋｓにより復号化して、カード１１０の公開暗号化キーＫＰｃａｒｄ（１）を復号抽出する（ステップＳ３３０）。

【０１１５】

続いて、カード１１２においては、メモリ１４１２からカード１１２の公開暗号化キーＫｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅが読出される（ステップＳ３３２）。

【０１１６】

続いて、カード１１２の復号処理部１４１６が、キーデータＫｃａｒｄ（２）

により、ライセンスキーＫｃ、データＬｉｃｅｎｓｅを復号処理する（ステップＳ３３４）。

【０１１７】

カード１１２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

【０１１８】

さらに、カード１１２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたカード１１０における公開暗号化キーＫＰｃａｒｄ（１）により、キーデータＫｃ、データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

【０１１９】

カード１１２の暗号化処理部１４１４により暗号化されたデータは、切換スイッチ１４０８（接点Ｐｃが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をセッションキーＫｓにより暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを生成する（ステップＳ３４０）。

【０１２０】

続いて、メモリカード１１２は、携帯電話機１０２に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを出力し（ステップＳ３４２）、携帯電話機１０２はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを携帯電話機１００に対して送信する（ステップＳ３４４）。

【０１２１】

携帯電話機１００が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓは（ステップＳ３４６）、メモリカード１１０に対して伝達され、メモリカード１１０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受理する（ステップＳ３４８）。

【０１２２】

カード１１０においては、復号処理部１４１０により、セッションキーＫｓに

基づいて復号化処理されたデータをメモリ１４１２に格納する（ステップＳ３５０）。さらに、カード１１０においては、復号処理部１４１６が、キーデータＫｃａｒｄ（１）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステップＳ３５２）。

【０１２３】

復号されたライセンス情報データＬｉｃｅｎｓｅのレジスタ１５００への格納が終了すると、メモリカード１１０は携帯電話１００に移動受理を通知し、携帯電話１００は、携帯電話１０２に対して移動受理を送信する（ステップＳ３５４）。

【０１２４】

携帯電話１０２は、携帯電話１００からの移動受理を受信すると、メモリカード１１２に対してこれを転送し、メモリカード１１２は、これに応じて、レジスタ１５００に格納されたライセンス情報データ１５００を消去する（ステップ３５８）。

【０１２５】

一方、携帯電話１０２では、移動受理が受信されたことに応じて、ディスプレイ１１１０上に、ユーザ２に対して、メモリカード１１２のメモリ１４１２内に格納されている移動データに対応する記憶データの消去を行なって良いかを問うメッセージを表示する。これに応じて、ユーザ２は、キーボード１１０８からこのメッセージに対する回答を入力する（ステップＳ３６０）。

【０１２６】

レジスタ１５００内のデータの消去が完了し（ステップＳ３５８）、かつ、上記メッセージに対する回答の入力が行なわれると（ステップＳ３６０）、メモリカード１１２内のコントローラ１４２０は、メモリ１４１２内のデータの消去を行なうかの判断を行う（ステップＳ３６２）。

【０１２７】

メモリ１４１２内の該当データの消去が指示されている場合（ステップＳ３６２）、コントローラ１４２０により制御されて、メモリ１４１２内のデータ［D

ｃ］Ｋｃおよびデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が消去され（ステップＳ３６４）、処理が終了する（ステップＳ３７４）。

【０１２８】

一方、メモリ１４１２内の該当データの消去が指示されていない場合（ステップＳ３６２）、処理は終了する（ステップＳ３７４）。この場合、メモリ１４１２内には、データ［Ｄｃ］Ｋｃおよびデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が残っていることになるが、レジスタ１５００内にライセンス情報データが存在しないため、ユーザ２は、再度、サーバ３０から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、カード１１２は「状態ＳＢ」となる。カード１１０においては、暗号化されたコンテンツデータ以外にも、ライセンスキーデータＫｃ、ライセンス情報データが移動されているので、カード１１０は「状態ＳＡ」となっている。

【０１２９】

一方、ステップＳ３０６′において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機１００から携帯電話機１０２に対して複製受理が送信される（ステップＳ３７０）。携帯電話機１０２において、複製受理を受信すると（ステップＳ３７２）、処理が終了する（ステップＳ３７４）。

【０１３０】

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化キーＫＰｍｅｄｉａ（１）およびＫＰｍｅｄｉａ（２）を送信した上で、移動動作を行うこと、および複製動作を行なうことが可能となる。

【０１３１】

［実施の形態２］

実施の形態２のデータ配信システムにおいては、実施の形態１のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを１つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをキーＫｓとし、一方のメモリカード１２０の発生するセッションキーをキーＫｓ１とし、メ

モリカード１２０と同様の構成を有する他方のメモリカード１２２の発生するセッションキーをキーＫｓ２とする。

【０１３２】

すなわち、実施の形態２のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を１つの特徴とするものである。

【０１３３】

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化キーをＫＰｐとし、このキーＫＰｐで暗号化されたデータを復号化できる秘密復号キーをキーＫｐとする。

【０１３４】

図１１は、実施の形態２のメモリカード１２０に対応した音楽サーバ３１の構成を示す概略ブロック図である。図３に示した音楽サーバ３０の構成と異なる点は、データ処理部３１０における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓにより暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、キーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介して通信装置３５０に与える点である。

【０１３５】

音楽サーバ３１のその他の点は、図３に示した実施の形態１の音楽サーバ３０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１３６】

図１２は、実施の形態２における携帯電話機１０１の構成を説明するための概略ブロック図である。

【０１３７】

図４に示した携帯電話機１００の構成と異なる点は、まず、メモリカード１２０が装着されていること以外に、携帯電話機１０１は、公開暗号化キーＫＰｐを保持して、再生動作時にキーＫＰｐをデータバスＢＳ２に出力するＫＰｐ保持部１５２４を備える構成となっていることである。

【０１３８】

さらに、携帯電話機１０１は、秘密復号キーＫｐを保持するＫｐ保持部１５２０と、このＫｐ保持部１５２０から与えられるキーＫｐに基づいて、データバスＢＳ２を介してメモリカード１２０から与えられるキーＫＰｐで暗号化されたセッションキーＫｓ１を復号し抽出する復号処理部１５２２とをさらに備える構成となっている。しかも、暗号化処理部１５０４は、この復号処理部１５２２から与えられるセッションキーＫｓ１により、Ｋｓ発生部１５０２からの自身のセッションキーＫｓを暗号化してデータバスＢＳ２に出力する。

【０１３９】

携帯電話機１０１のその他の点は、図４に示した実施の形態１の携帯電話機１００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１４０】

図１３は、本発明の実施の形態２のメモリカード１２０の構成を説明するための概略ブロック図であり、実施の形態１の図５と対比される図である。

【０１４１】

メモリカード１２０の構成が、メモリカード１１０の構成と異なる点は、まず、メモリカード１２０は、このカード独自のセッションキーＫｓ１を発生するセッションキーＫｓ１発生部１４３２を備えることである。

【０１４２】

さらに、メモリカード１２０は、セッションキー発生回路１４３２で生成されたセッションキーＫｓ１を、暗号化してデータバスＢＳ３に与えるための暗号化

処理部１４３０を備える。

【０１４３】

これに応じて、メモリカード１２０は、さらに、移動動作において、相手方（移動先）の公開暗号化キーＫＰｍｅｄｉａ（ｎ）を受けて保持するＫＰｍｅｄｉａ受理部１４０３と、このＫＰｍｅｄｉａ受理部１４０３の出力と、再生動作においてデータバスＢＳ３を介して携帯電話機１０１から与えられる公開暗号化キーＫＰｐとを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ１４３６を備える。切換えスイッチ１４３６は、接点ＰｉおよびＰｈとを有し、接点ＰｉはデータバスＢＳ３と、接点ＰｈはＫＰｍｅｄｉａ受理部１４０３とそれぞれ結合する。暗号化処理部１４３０は、切換えスイッチ１４３６から与えられるキーＫＰｍｅｄｉａ（ｎ）またはキーＫＰｐのいずれかにより、Ｋｓ１発生部１４３２からのセッションキーＫｓ１を暗号化して、データバスＢＳ３に与える。

【０１４４】

すなわち、切換えスイッチ１４３６は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点Ｐｉの側に閉じており、移動動作において移動元となっているときは、接点Ｐｈの側に閉じている。

【０１４５】

メモリカード１２０は、さらに、接点Ｐｅ、ＰｆおよびＰｇを有し、復号処理部１４０４から与えられる配信サーバからのセッションキーＫｓと、Ｋｓ１発生部１４３２の出力と、データバスＢＳ４から与えられる携帯電話機１０１からのセッションキーＫｓとを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４３５を備える。接点Ｐｅには復号処理部１４０４からの出力が、接点ＰｆにはＫｓ１発生部１４３２の出力が、接点Ｐｇにはデータバスバス４がそれぞれ結合している。したがって、暗号化処理部１４０６と復号処理部１４１０は、この切換えスイッチ１４３５から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行う。

【０１４６】

すなわち、切換えスイッチ１４３５は、配信動作の場合に配信サーバ３１からのセッションキーの抽出を行なうときは、接点Ｐｅの側に閉じており、配信動作の場合に配信サーバ３１からの暗号化されたライセンスキーＫｃ、ライセンス情報データについてキーＫｓ１による復号を行なうときは、接点Ｐｆの側に閉じている。切換えスイッチ１４３５は、再生動作において復号処理を行うときは、接点Ｐｆの側に閉じており、再生動作において暗号化処理を行うときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動動作において移動元となっている場合に復号処理を行うときは、接点Ｐｆの側に閉じており、移動動作において移動元となっている場合に暗号化処理を行うときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点Ｐｅの側に閉じており、移動動作において移動先となっている場合にライセンスキーKcおよびライセンス情報データを受け取るときは、接点Ｐｆの側に閉じている。

【０１４７】

メモリカード１２０は、さらに、接点Ｐａ、Ｐｂ、ＰｃおよびＰｄ　を有し、Ｋｓ１発生部１４３２から与えられる自身のセッションキーＫｓ１と、ＫＰｃａｒｄ保持部１４０５の出力と、データバスＢＳ５から与えられるライセンスキーＫｃと、暗号化処理部１４１４から与えられ、相手方の公開暗号化キーＫＰｃａｒｄ（ｎ）により暗号化されたライセンスキーＫｃおよびライセンス情報データを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４０９を、切換えスイッチ１４０８の替わりに備える。

【０１４８】

接点ＰａにはＫｓ１発生部１４３２からの出力が、接点ＰｂにはＫＰｃａｒｄ（１）保持部１４０５の出力が、接点ＰｃにはデータバスＢＳ５が、接点Ｐｄには暗号化処理部１４１４の出力が、それぞれ結合している。したがって、暗号化処理部１４０６は、この切換えスイッチ１４０９から与えられるデータに対して、それぞれ、暗号化処理を行う。

【０１４９】

すなわち、切換えスイッチ１４０９は、配信動作において、配信先となってい

る場合にサーバ３１に自身の公開暗号化キーＫＰｃａｒｄ（１）や自身のセッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。切換えスイッチ１４０９は、再生動作のときは、接点Ｐｃの側に閉じており、移動動作において移動元となっているときは、接点Ｐｄの側に閉じている。切換えスイッチ１４０９は、移動動作において移動先となっている場合にも移動元に自身の公開暗号化キーＫＰｃａｒｄ（１）や自身のセッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。

【０１５０】

図１４および図１５は、図１３で説明したメモリカード１２０を用いた配信動作を説明するための第１および第２のフローチャートである。

【０１５１】

図６および図７においても、ユーザ１が、メモリカード１１０を用いることで、音楽サーバ３０から音楽データの配信を受ける場合の動作を説明している。

【０１５２】

まず、ユーザ１の携帯電話機１０１から、ユーザによりキーボード１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【０１５３】

カード１２０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化キーＫＰｍｅｄｉａ（１）をサーバ３１に対して送信する（ステップＳ１０２）。さらに、カード１２０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ１０９）。

【０１５４】

サーバ３１では、カード１２０から転送された配信リクエストならびにキーＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０４）、受信したキーＫＰｍｅｄｉａ（１）に基づいて、認証サーバ１２に対して照会を行ない、正規ユーザからのアクセスの場合は次の処理に移行し（ステップＳ１０６）、正規ユーザでない場合には、処理を終了する（ステップＳ１５４）。

【０１５５】

照会の結果、正規ユーザであることが確認されると、サーバ３１では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、サーバ３１内の暗号化処理部３１６が、受信したキーＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化してデータ［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

【０１５６】

続いて、サーバ３１は、データ［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化データ［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１０１のメモリカード１２０に対して送信する（ステップＳ１１０）。

【０１５７】

携帯電話機１０１が、データ［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１２０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、キーデータＫｍｅｄｉａ（１）で復号処理することにより、セッションキーデータＫｓを復号し抽出する（ステップＳ１１４）。

【０１５８】

続いて、配信動作においては、切換スイッチ１４０９は、接点ＰａまたはＰｂが順次閉じる状態が選択されるので、暗号化処理部１４０６は、接点Ｐａを介してセッションキー発生部１４３２から与えられるセッションキーＫｓ１と接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１２０に対する公開暗号化鍵）とを、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ１１８）。

【０１５９】

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓをサーバ３１に対して送信する（ステップＳ１２０）。

【０１６０】

サーバ３１では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、キーデータＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ１２４）。

【０１６１】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

【０１６２】

さらに、サーバ３１は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１２０に送信する（ステップＳ１２８）。

【０１６３】

携帯電話機１０１がデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１２０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

【０１６４】

一方、サーバ３１は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのキーデータＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられたキーデータＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

【０１６５】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらに、メモリカード１２０からのセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ

，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１をカード１２０に対して送信する。

【０１６６】

携帯電話１０１がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ１４２）、カード１２０においては、復号処理部１４１０が接点Ｐｆを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ１４６）。

【０１６７】

さらに、カード１２０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

【０１６８】

以上のような動作により、メモリカード１２０自身が、暗号化コンテンツデータを送る側（サーバ３１）に、公開暗号化キーＫＰｍｅｄｉａ（１）およびセッションキーＫｓ１を送信した上で、配信を受けることができ、メモリカード１２０は、音楽情報を再生可能な状態となる。

【０１６９】

さらに、メモリカード１２０からサーバ３１へは、配信受理が通知され、サーバ３１で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

【０１７０】

図１６および図１７は、携帯電話１０１内において、メモリカード１２０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明する第１および第２のフローチャートである。

【０１７１】

図１６および図１７を参照して、携帯電話のキーボード１１０８等からのユー

ザ１の指示により、再生リクエストがメモリカード１２０に対して出力される（ステップＳ２００）。

【０１７２】

カード１２０においては、この再生リクエストに応じて、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、復号可能と判断した場合は、再生可能通知を携帯電話１０１に対して送信する（ステップＳ２４０）。一方、復号不可能と判断した場合は、処理を終了する（ステップＳ２８０）。

【０１７３】

復号可能と判断され、カード１２０から再生可能通知が送信された場合、携帯電話１０１では、公開暗号化キーＫＰｐをカード１２０に送信し（ステップＳ２４２）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成する（ステップＳ２４４）。

【０１７４】

一方、メモリカード１２０も、セッションキーＫｓ１を生成する（ステップＳ２４０）。メモリカード１２０は、さらに、データバスＢＳ２を介して携帯電話機から受けとったキーＫＰｐによりセッションキーＫｓ１を暗合化し（ステップＳ２４８）、生成されたデータ［Ｋｓ１］Ｋｐを携帯電話１０１に対して送信する（ステップＳ２５０）。

【０１７５】

携帯電話１０１では、メモリカード１２０からのデータ［Ｋｓ１］Ｋｐを受信すると、復号処理部１５２２が、キーＫｐにより復号化してメモリカード１２０で生成したセッションキーＫｓ１を抽出する（ステップＳ２５２）。続いて、携帯電話１０１の暗号化処理部１５０４は、携帯電話１０１で生成したセッションキーＫｓをキーＫｓ１により暗号化して、データ［Ｋｓ］Ｋｓ１を生成し（ステップＳ２５４）、このデータ［Ｋｓ］Ｋｓ１をメモリカード１２０に対して送信する（ステップＳ２５６）。

【０１７６】

メモリカード１２０は、データバスＢＳ２を介して、携帯電話機により生成され、かつ暗号化されたセッションキーＫｓを受け取り、セッションキーＫｓ１により復号し、携帯電話１０１で生成したセッションキーＫｓを抽出する（ステップＳ２５８）。

【０１７７】

続いて、メモリカード１２０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読出し、復号処理部１４１６が復号処理を行なう（ステップＳ２６０）。

【０１７８】

キーＫｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２６２）、ライセンスキーＫｃが抽出される（ステップＳ２６４）。　一方、復号不可能の場合、処理は終了する（ステップＳ２８０）。

【０１７９】

メモリ１４１２から読み出されたデータを復号可能な場合は、さらに、レジスタ１５００内のライセンス情報データのうち、再生回数に関するデータが変更される（ステップＳ２６６）。

【０１８０】

続いて、メモリカード１２０においては、暗合化処理部１４０６が、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２６８）、暗号化されたライセンスキー［Ｋｃ］Ｋｓをデータバスバス２に与える（ステップＳ２７０）。

【０１８１】

携帯電話機１０１の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２７２）。

【０１８２】

続いて、メモリカード１２０は、暗号化されたコンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２７４）

【０１８３】

携帯電話機の音楽再生部１５０８は、暗号化されたコンテンツデータ［Ｄｃ］Ｋｃを、抽出されたキーデータＫｃにより復号処理して平文の音楽データを生成し（ステップＳ２７６）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ２７６）。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

【０１８４】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキーＫｓ１またはＫｓを生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行うことが可能となる。

【０１８５】

図１８および図１９は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

【０１８６】

まず、携帯電話１０１と同様の構成を有する携帯電話機１０３が送信側であり、携帯電話機１０１が受信側であるものとする。また、携帯電話機１０３にも、メモリカード１２０と同様の構成を有するメモリカード１２２が装着されているものとする。

【０１８７】

携帯電話機１０３は、まず、自身の側のメモリカード１２２および携帯電話１０１に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

【０１８８】

カード１２２は、これに応じて、メモリ１４１２内のデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１２０に対して出力し（ステップＳ３０２）、一方、携帯電話１０１は、携帯電話機１０３からのリクエストを受信し（ステップＳ３０

１）、メモリカード１２０では、データ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

【０１８９】

続いて、携帯電話１０３および１０１においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６′）、「移動リクエスト」である場合、カード１２０は、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１０１に出力し（ステップＳ３０８）、携帯電話１０１は、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１０３に対して送信する（ステップＳ３１０）。

【０１９０】

携帯電話機１０３が、キーＫＰｍｅｄｉａ（１）を受信し（ステップＳ３１２）、メモリカード１２２に転送すると（ステップＳ３１３）、メモリカード１２２のＫｓ２発生回路１４３２は、セッションキーＫｓ２を生成し（ステップＳ３１４）、公開暗号化キーＫＰｍｅｄｉａ（１）を用いて、暗号化処理部１４３０がセッションキーＫｓ２を暗号化する（ステップＳ３１５）。

【０１９１】

携帯電話機１０３は、暗号化されたセッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を携帯電話機１０１に対して送信する（ステップＳ３１６）。携帯電話機１０１は、データ［Ｋｓ２］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、カード１２０に伝達し、カード１２０は、復号処理部１４０４が復号して、セッションキーＫｓ２を受理する（ステップＳ３２０）。

【０１９２】

カード１２０においては、セッションキーＫｓ２によりカード１２０の公開暗号化キーＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化して（ステップＳ３２２）、携帯電話機１０１から携帯電話機１０３に対して暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を送信する（ステップＳ３２４）。携帯電話機１０３は、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を受信し（ステップＳ３２６）、カード１２２に転送する。

【０１９３】

カード１２２においては、復号処理部１４１０が、カード１２０から送信された暗号化データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２をセッションキーＫｓ２により復号化して、カード１２０の公開暗号化キーＫＰｃａｒｄ（１）、セッションキーＫｓ１を復号抽出する（ステップＳ３３０）。

【０１９４】

続いて、カード１２２においては、メモリ１４１２からカード１２２の公開暗号化キーＫｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅが読出される（ステップＳ３３２）。

【０１９５】

続いて、カード１２２の復号処理部１４１６が、キーデータＫｃａｒｄ（２）により、ライセンスキーＫｃ、データＬｉｃｅｎｓｅを復号処理する（ステップＳ３３４）。

【０１９６】

カード１２２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

【０１９７】

さらに、カード１２２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたカード１２０における公開暗号化キーＫＰｃａｒｄ（１）により、キーデータＫｃ、データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

【０１９８】

カード１２２の暗号化処理部１４１４により暗号化されたデータは、切換スイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、メモリカード１２２の暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をセッションキーＫｓ１により暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を生成する（ステップＳ３４０）。

【０１９９】

続いて、メモリカード１２２は、携帯電話機１０３に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を出力し（ステップＳ３４２）、携帯電話機１０３はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を携帯電話機１０１に対して送信する（ステップＳ３４４）。

【０２００】

携帯電話機１０１が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１は（ステップＳ３４６）、メモリカード１２０に対して伝達され、メモリカード１２０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受理する（ステップＳ３４８）。

【０２０１】

カード１２０においては、復号処理部１４１０により、セッションキーＫｓ１に基づいて復号化処理されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をメモリ１４１２に格納する（ステップＳ３５０）。さらに、カード１２０においては、復号処理部１４１６が、キーデータＫｃａｒｄ（１）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステップＳ３５２）。

【０２０２】

以後の移動動作における処理ならびに複製動作におけるメモリカード１２０および１２２の処理は、図９および図１０で説明した実施の形態１のメモリカード１１０、１１２等の処理と同様であるので、その説明は繰り返さない。

【０２０３】

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動動作を行うこと、および複製動作を行なうことが可能となる。

【０２０４】

したがって、データバス上等で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティーが一層

向上するという効果がある。

【０２０５】

しかも、以上のような構成を用いることで、たとえば、メモリカード１２２からメモリカード１２０へのデータの移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインターフェース機器により行うことも可能となり、ユーザの利便性が一層向上するという効果がある。

【０２０６】

ここで、移動時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ１４１２に記録されたライセンス情報データを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンス情報データに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【０２０７】

［実施の形態３］

実施の形態３のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社２０から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを１つの特徴とする。

【０２０８】

図２０は、このような実施の形態３のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機１００およびメモリカード１１０の構成は実施の形態１で説明したものと同様であるので、その説明は繰り返さない。

【０２０９】

図２０を参照して、コンテンツデータ販売機２０００は、ユーザに対して配信作業における案内等を出力するためのディスプレイ２００２と、ユーザから指示を入力するためのキーボード２００４と、料金投入口２００６と、携帯電話１０

０とコネクタ１１２０を介してデータの授受を行うための外部コネクタ２０１０とを備える。さらに、コンテンツデータ販売機２０００は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ２２００と接続している。

【０２１０】

図２１は、実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。コンテンツデータ販売機２０００は、上述したように、ディスプレイ２００２と、キーボード２００４と、料金投入口２００６からの投入金を受ける料金受理部２０２０と、外部コネクタ２０１０と、コネクタ２０１０とデータバスとの間に設けられるインターフェース部２０１２と、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース３０４と、管理サーバ２２００との間で情報の授受をするための通信装置３６０と、配信情報データベース３０４および管理サーバ２２００からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部２１００とを備える。

【０２１１】

データ処理部２１００中は、実施の形態１と同様に、データバスＢＳ１上のデータに応じて、データ処理部２１００の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、カード媒体に固有な公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）により暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話においてセッションキーＫｓにより暗号化されたうえでコネクタ２０１０から与えられたデータをデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンス情報データを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１を介してコネクタ２０１０に与える暗号化処理部３２２とを含む。

【０２１２】

図２２および図２３は、図２０および図２１で説明したデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【０２１３】

図２２および図２３においては、ユーザ１が、メモリカード１１０を用いることで、コンテンツデータ販売機２０００から音楽データの配信を受ける場合の動作を説明している。

【０２１４】

まず、ユーザが、コンテンツデータ販売機２０００のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ４００）。販売機２０００は、カード１１０に対して公開暗号化キーＫＰｍｅｄｉａ（１）の送信依頼を出力する（ステップＳ４０２）。

【０２１５】

カード１１０においては、この公開暗号化キーＫＰｍｅｄｉａ（１）の送信依頼に応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化キーＫＰｍｅｄｉａ（１）を携帯電話機１００に対して出力する（ステップＳ４０６）。

【０２１６】

携帯電話１００が販売機２０００にキーＫＰｍｅｄｉａ（１）を送信し（ステップＳ４０８）、販売機２０００が、カード１１０から転送されたキーＫＰｍｅｄｉａ（１）を受信すると（ステップＳ４１０）、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ４１２）。続いて、販売機２０００は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、販売機２０００内の暗号化処理部３１６が、受信したキーＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化してデータ［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ４１４）。

【０２１７】

続いて、販売機２０００は、データ［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、コネクタ２０１０から出力する（ステップＳ４１６）。携帯電話機１００は、このデータ［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると、メモリカード１１０に転送する（ステップＳ４１８）。

【０２１８】

メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データ［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、キーデータＫｍｅｄｉａ（１）により復号処理することにより、セッションキーデータＫｓを復号し抽出する（ステップＳ４２０）。

【０２１９】

続いて、配信動作においては、切換スイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を、セッションキーＫｓにより暗号化し（ステップＳ４２２）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ４２４）。

【０２２０】

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓを販売機２０００に対して送信する（ステップＳ４２６）。

【０２２１】

販売機２０００では、コネクタ２０１０を介してデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ４２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、キーデータＫＰｃａｒｄ（１）を復号抽出する（ステップＳ４３０）。

【０２２２】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ４３２）。

【０２２３】

さらに、販売機２０００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、コネクタ２０１０を介して、携帯電話機１００に送信する（ステップＳ４３４）。

【０２２４】

携帯電話機１００がデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ４３６）、メモリカード１１０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ４３８）。

【０２２５】

一方、販売機２０００は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ４４０）、暗号化処理部３２０は、配信制御部３１２からのキーデータＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられたキーデータＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ４４２）。

【０２２６】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓがカード１１０に対して送信される（ステップＳ４４６）。

【０２２７】

携帯電話１００がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを受信すると（ステップＳ４４８）、カード１１０においては、復号処理部１４１０がセッションキーＫｓにより復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ４５２）。

【０２２８】

さらに、カード１１０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップＳ４５８）。

【０２２９】

以上のような動作により、メモリカード自身が、セッションキーＫｓを送る側

（販売機２０００）に、公開暗号化キーＫＰｍｅｄｉａ（１）を送信した上で、配信を受けることができ、メモリカード１１０は、音楽情報を再生可能な状態となる。

【０２３０】

さらに、メモリカード１１０から販売機２０００へは、携帯電話機１００を介して配信受理が通知され（ステップＳ４６０）、販売機２０００で配信受理を受信すると（ステップＳ４６２）、管理サーバに販売記録が送信され（ステップＳ４６４）、処理が終了する（ステップＳ４６６）。

【０２３１】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

【０２３２】

［実施の形態３の変形例］

実施の形態３のデータ配信システムにおいては、メモリカード１１０は、携帯電話１００を介して、コンテンツデータ販売機２０００から暗号化コンテンツデータの配信を受ける構成であった。

【０２３３】

しかしながら、図２１に示した販売機２０００の構成において、コネクタ２０１０の代わりに、メモリカード１１０との間のインターフェースのためのメモリスロットを設ける構成とすれば、携帯電話１００を介することなく、メモリカード１１０と販売機２０００とが直接データの授受を行うことが可能である。

【０２３４】

図２４は、このような実施の形態３の変形例のコンテンツデータ販売機２００１の構成を示す概念図である。図２０に示した実施の形態３の販売機２０００の構成と異なる点は、外部コネクタ２０１０の代わりに、メモリカードを挿入できるカードスロット２０３０が設けられ、このカードスロット２０３０がインターフェース部２０１２を介して、データバスＢＳ１とデータの授受をする構成となっている点である。

【０２３５】

図２５および図２６は、実施の形態３の変形例のデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【０２３６】

図２２および図２３に示した実施の形態３の配信動作とは、携帯電話１００を介さずに、メモリカード１１０と販売機２００１がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【０２３７】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【０２３８】

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽データの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【０２３９】

［実施の形態４］

図２７は、実施の形態４のコンテンツデータ販売機３０００の構成を説明するための概略ブロック図である。図２１に示したコンテンツデータ販売機２０００の構成と異なる点は、対象となるメモリカードが実施の形態２のメモリカード１２０であり、かつ使用される端末が携帯電話１０１である点、およびこれに対応して、データ処理部２１００における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓにより暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、キーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介してインターフェース部２０１２およびコネクタ２０１０に与える点である。

【０２４０】

コンテンツデータ販売機３０００のその他の点は、図２１に示した実施の形態３のコンテンツデータ販売機２０００の構成の構成と同様であるので、同一部分

には同一符号を付してその説明は繰り返さない。

【０２４１】

また、携帯電話１０１およびメモリカード１１０の構成も実施の形態２で説明したものと同様であるので、その説明も繰り返さない。

【０２４２】

図２８および図２９は、図２７で説明したデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【０２４３】

図２８および図２９においては、ユーザ１が、メモリカード１２０を用いることで、コンテンツデータ販売機３０００から音楽データの配信を受ける場合の動作を説明している。

【０２４４】

まず、ユーザが、コンテンツデータ販売機３０００のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ５００）。販売機２０００は、カード１１０に対して公開暗号化キーＫＰｍｅｄｉａ（１）の送信依頼を出力する（ステップＳ５０２）。

【０２４５】

カード１２０においては、この公開暗号化キーＫＰｍｅｄｉａ（１）の送信依頼に応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化キーＫＰｍｅｄｉａ（１）を販売機３０００に対して送信する（ステップＳ５０６）。さらに、カード１２０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ５１５）。

【０２４６】

携帯電話１０１が販売機３０００にキーＫＰｍｅｄｉａ（１）を送信し（ステップＳ５０８）、販売機３０００が、カード１２０から転送されたキーＫＰｍｅｄｉａ（１）を受信すると（ステップＳ５１０）、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ５１２）。続いて、販売機３０００は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、販売機３０００内の暗号化処理部３１６が、受信したキーＫＰ

ｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化してデータ［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ５１４）。

【０２４７】

続いて、販売機３０００は、データ［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、コネクタ２０１０から出力する（ステップＳ４１６）。携帯電話機１０１は、このデータ［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると、メモリカード１２０に転送する（ステップＳ５１８）。

【０２４８】

メモリカード１２０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データ［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、キーデータＫｍｅｄｉａ（１）により復号処理することにより、セッションキーデータＫｓを復号し抽出する（ステップＳ５２０）。

【０２４９】

続いて、暗号化処理部１４０６は、ＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）およびＫｓ１発生部１４３２からのセッションキーＫｓ１を、セッションキーＫｓにより暗号化し（ステップＳ５２２）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ５２４）。

【０２５０】

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを販売機３０００に対して送信する（ステップＳ５２６）。

【０２５１】

販売機３０００では、コネクタ２０１０を介してデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ５２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、キーデータＫＰｃａｒｄ（１）およびキーＫｓ１を復号抽出する（ステップＳ５３０）。

【０２５２】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ５３２）。

【０２５３】

さらに、販売機３０００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、コネクタ２０１０を介して、携帯電話機１０１に送信する（ステップＳ５３４）。

【０２５４】

携帯電話機１０１がデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ５３６）、メモリカード１２０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ５３８）。

【０２５５】

一方、販売機３０００は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ５４０）、暗号化処理部３２０は、配信制御部３１２からのキーデータＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられたキーデータＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ５４２）。

【０２５６】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１が携帯電話１０１に対して出力される（ステップＳ５４６）。

【０２５７】

携帯電話１０１がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ５４８）、カード１２０においては、復号処理部１４１０がセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ５５２）。

【０２５８】

以下の処理は、図２２および図２３に示した実施の形態３の処理と同様であるので、その説明は繰り返さない。

【０２５９】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

【０２６０】

しかも、データバス上等で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティーが一層向上するという効果がある。

【０２６１】

［実施の形態４の変形例］

実施の形態４のデータ配信システムにおいては、メモリカード１２０は、携帯電話１０１を介して、コンテンツデータ販売機３０００から暗号化コンテンツデータの配信を受ける構成であった。

【０２６２】

しかしながら、図２７に示した販売機３０００の構成において、実施の形態３の変形例と同様に、コネクタ２０１０の代わりに、メモリカード１２０との間のインターフェースのためにメモリースロットを設ける構成とすれば、携帯電話１０１を介することなく、メモリカード１２０と販売機３０００とが直接データの授受を行うことが可能である。

【０２６３】

このような実施の形態４の変形例のコンテンツデータ販売機３００１の構成は、データ処理部２１００の構成を除いて、図２４に示した実施の形態３の変形例の構成と同様である。

【０２６４】

すなわち、実施の形態４の変形例のコンテンツデータ販売機３００１の構成は、図２７に示した実施の形態４の販売機３０００の構成と異なり、外部コネクタ２０１０の代わりに、メモリカードを挿入できるカードスロット２０３０が設け

られ、このカードスロット２０３０がインターフェース部２０１２を介して、データバスＢＳ１とデータの授受をする構成となっている。

【０２６５】

図３０および図３１は、実施の形態４の変形例のデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【０２６６】

図２８および図２９に示した実施の形態３の配信動作とは、携帯電話１０１を介さずに、メモリカード１２０と販売機３００１がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【０２６７】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【０２６８】

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽データの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【０２６９】

なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作情報や音楽サーバ３０に対するアクセス情報等を、付加情報Ｄｉとして暗号化コンテンツデータと併せて配信することも可能である。この付加データＤｉは、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されて音楽データとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ１４１２に記録される。

【０２７０】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範

囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０２７１】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、１度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

【０２７２】

また、ユーザが配信キャリアを介してではなく、販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上する。

【図面の簡単な説明】

【図１】　本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【図２】　図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

【図３】　図１に示した音楽サーバ３０の構成を示す概略ブロック図である。

【図４】　図１に示した携帯電話１００の構成を説明するための概略ブロック図である。

【図５】　図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【図６】　図１および図３～図５で説明したデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図７】　図１および図３～図５で説明したデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図８】　携帯電話１００内において音楽情報を復号化し、音楽として外部

に出力するための再生処理を説明するフローチャートである。

【図９】　２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

【図１０】　２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

【図１１】　実施の形態２のメモリカード１２０に対応した音楽サーバ３１の構成を示す概略ブロック図である。

【図１２】　実施の形態２における携帯電話機１０１の構成を説明するための概略ブロック図である。

【図１３】　本発明の実施の形態２のメモリカード１２０の構成を説明するための概略ブロック図である。

【図１４】　図１３で説明したメモリカード１２０を用いた配信動作を説明するための第１のフローチャートである。

【図１５】　図１３で説明したメモリカード１２０を用いた配信動作を説明するための第２のフローチャートである。

【図１６】　携帯電話１０１内において音楽情報を復号化し、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

【図１７】　携帯電話１０１内において音楽情報を復号化し、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

【図１８】　２つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

【図１９】　２つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

【図２０】　実施の形態３のデータ配信システムの構成を説明するための概念図である。

【図２１】　実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。

【図２２】　図２０および図２１で説明したデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図２３】　図２０および図２１で説明したデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図２４】　実施の形態３の変形例のコンテンツデータ販売機２００１の構成を示す概念図である。

【図２５】　実施の形態３の変形例のデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図２６】　実施の形態３の変形例のデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図２７】　実施の形態４のコンテンツデータ販売機３０００の構成を説明するための概略ブロック図である。

【図２８】　図２７で説明したデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図２９】　図２７で説明したデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図３０】　実施の形態４の変形例のデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図３１】　実施の形態４の変形例のデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

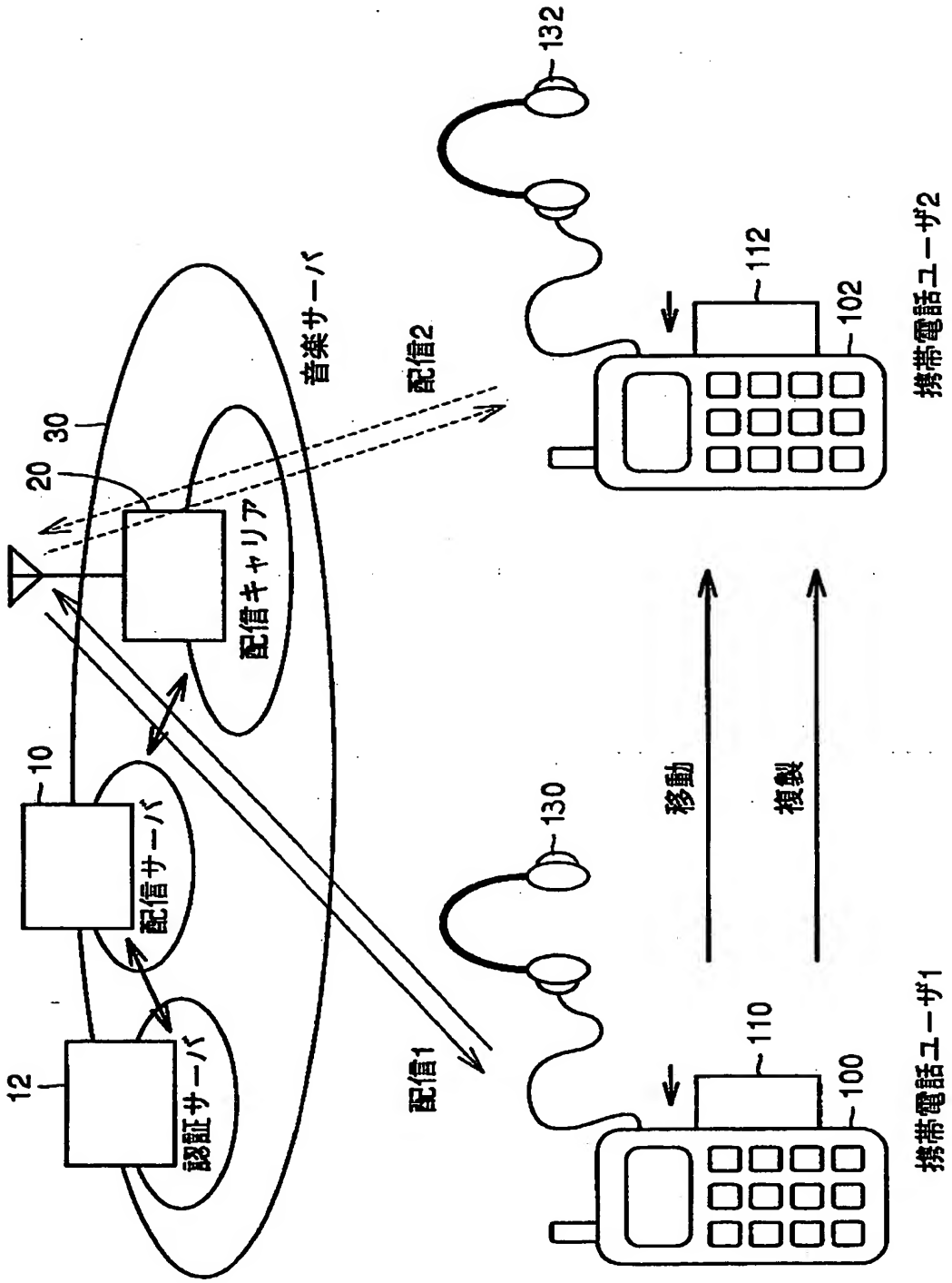
【符号の説明】

１０　コンテンツサーバ、２０　配信キャリア、３０，３１　音楽サーバ、１００，１０１，１０２，１０３　携帯電話機、１１０，１１２，１２０，１２２　メモリカード、１３０，１３２　ヘッドホン、１１０２　アンテナ、１１０４　送受信機、１１０６　コントローラ、１１０８　タッチキー部、１１１０　ディスプレイ、１１１２　音声再生部、１２００　メモリインタフェース、１４０４　復号処理部、１４０６　暗号化処理部、１４０８，１４０９　切替スイッチ、１４１０　復号処理部、１４１２　メモリ、１４１４　暗号化処理部、１４１６　復号処理部、１４２０　コントローラ、１４３０　暗号化処理部、１４３２

セッションキー発生部、１４３４，１４３５　切替スイッチ、１５０２　セッションキー発生部、１５０４　暗号化処理部、１５０６　復号処理部、１５０８　音楽再生部、１５１０　混合部、１５１２　デジタルアナログ変換器、２００，３０００　コンテンツデータ販売機。

【書類名】　　図面

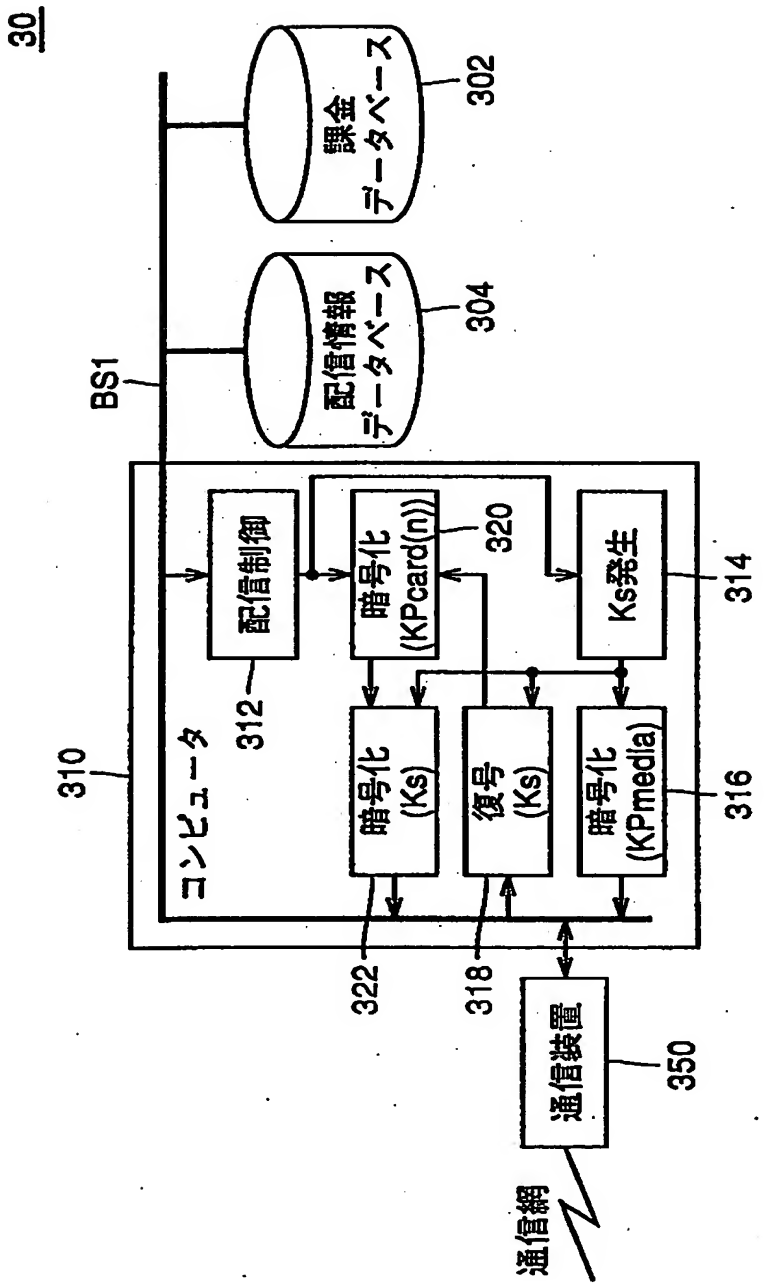
【図１】


132
112
102
携帯電話ユーザ2
音楽サーバ
配信2
30
20
配信キャリア
10
配信サーバ
12
認証サーバ
130
移動
複製
配信1
110
100
携帯電話ユーザ1

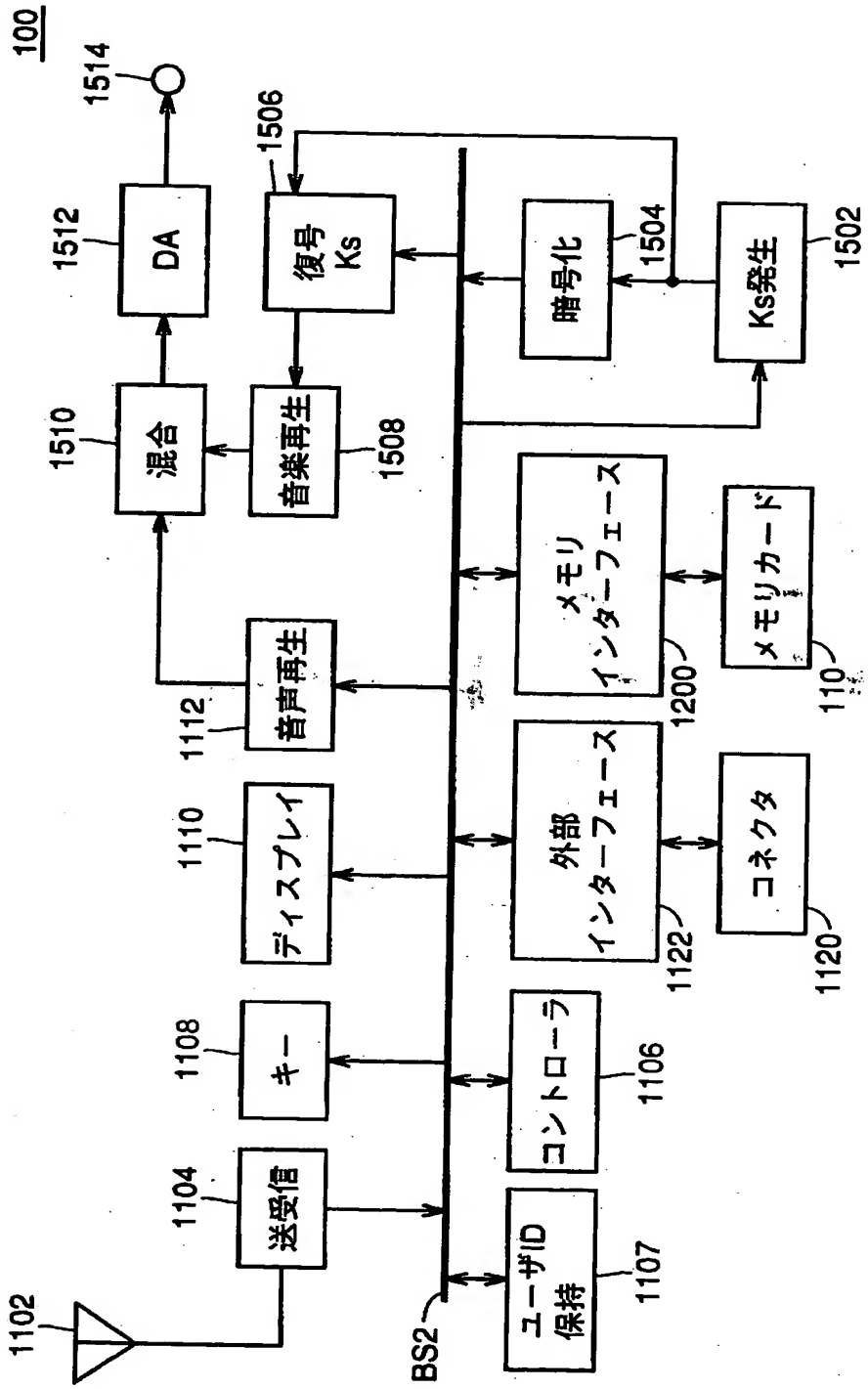
【図２】

	記号	属性	特性	
メモリカード内管理の鍵	Kmedia(n)	秘密復号鍵	媒体固有	メモリカードの種類ごとに固有な情報を有する
	Kcard(n)	秘密復号鍵		メモリカード毎に異なる
	KPcard(n)	公開暗号化鍵		Kcard(n)と対を成す。 KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション固有	通信毎（例：アクセス毎）に発生。 配信サーバ、携帯電話機にて管理
配信データ	Kc	共通鍵	ライセンスキー	暗号化コンテンツデータの復号鍵
	License-ID	再生に関する情報		例：曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別する情報		例：電話番号
	Dc	コンテンツデータ		例：音楽情報データ
	[Dc]Kc	暗号化コンテンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

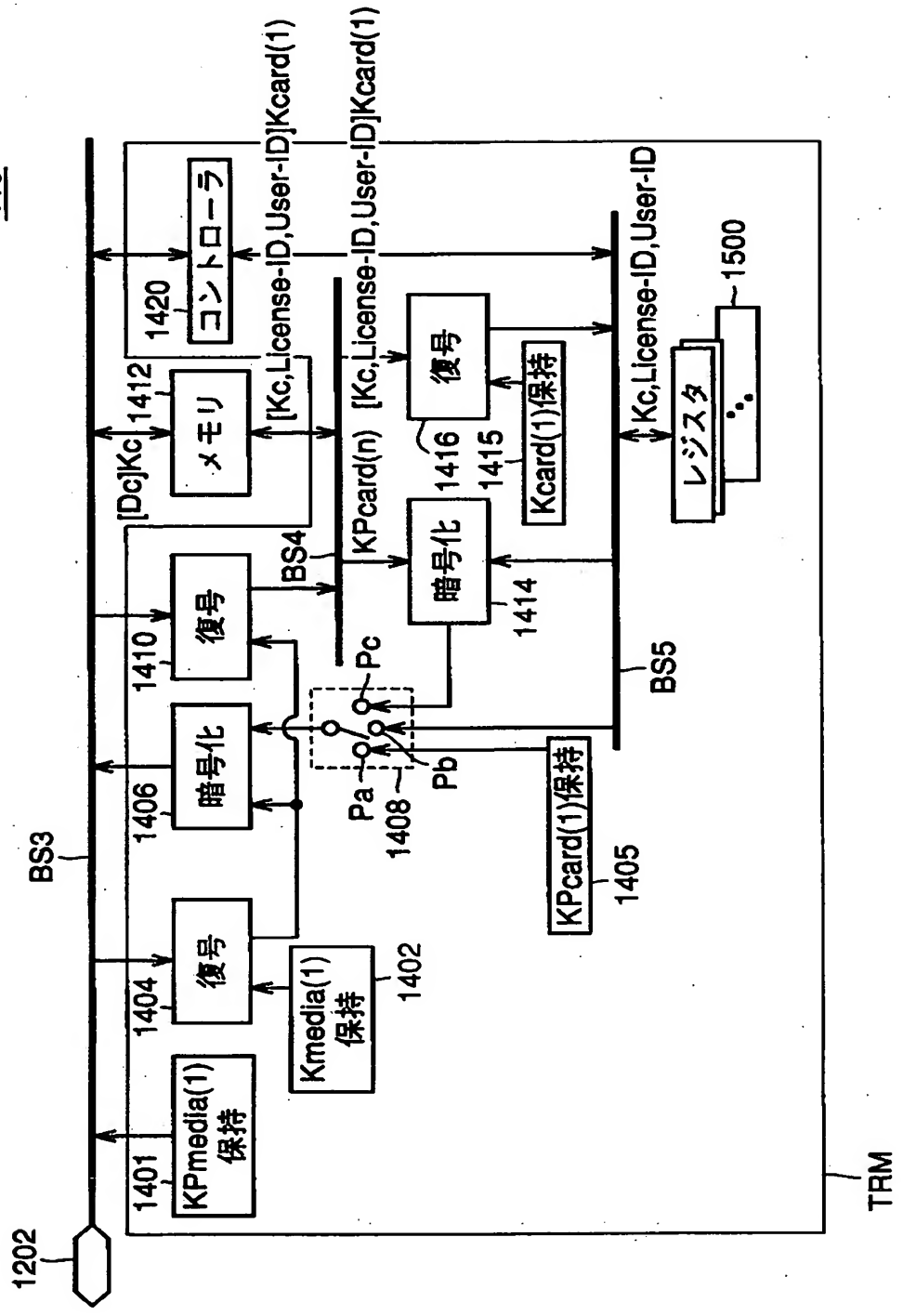
【図３】


30
課金データベース
302
配信情報データベース
304
BS1
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
コンピュータ
310
暗号化(Ks)
復号(Ks)
暗号化(KPmedia)
316
322
318
通信装置
350
通信網

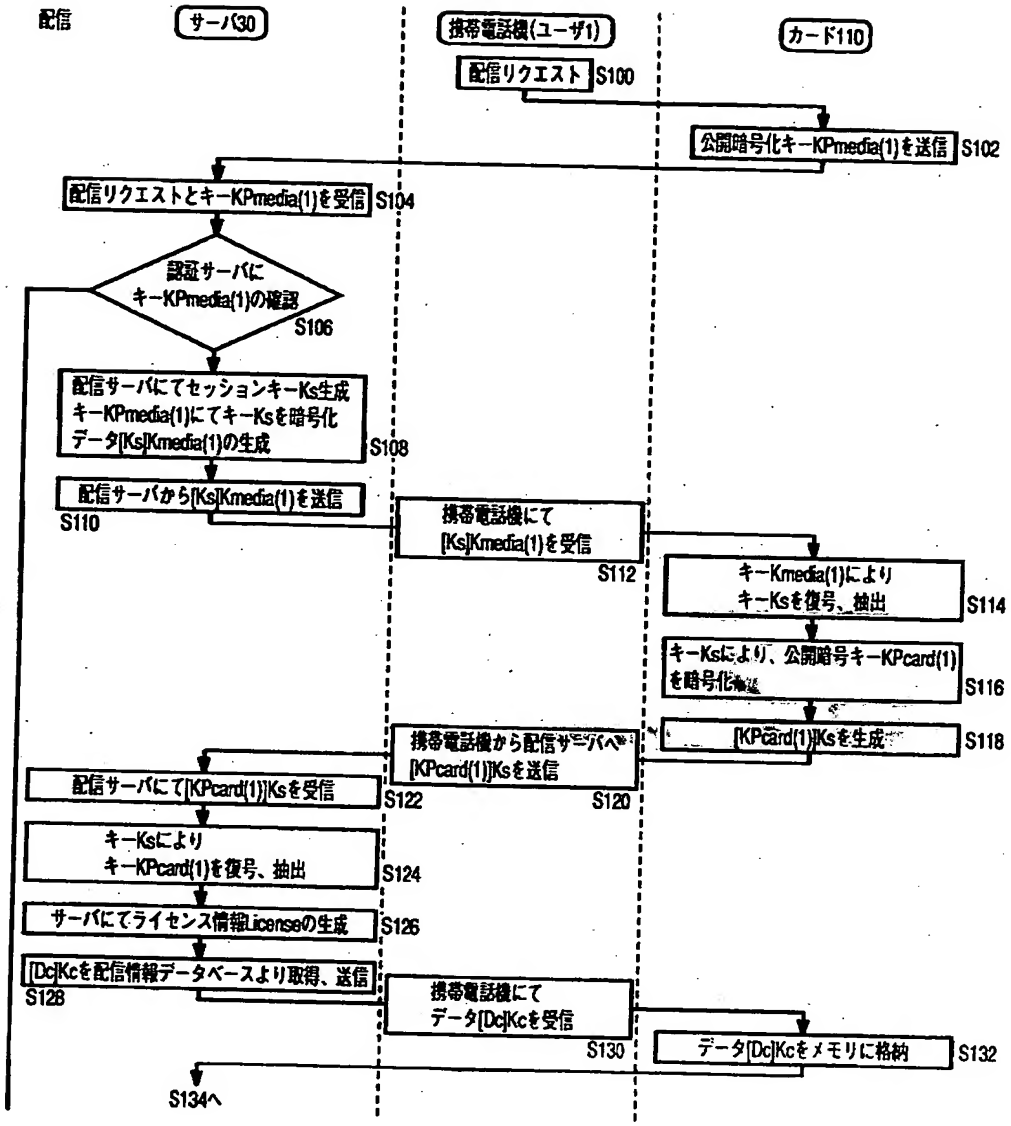
【図４】


100
1514
1506
1512
DA
復号
Ks
暗号化
1504
Ks発生
1502
1510
混合
音楽再生
1508
メモリ
インターフェース
メモリカード
1200
110
1112
音声再生
1110
ディスプレイ
外部
インターフェース
コネクタ
1122
1120
1108
キー
コントローラ
1106
1104
送受信
ユーザID
保持
1107
1102
BS2

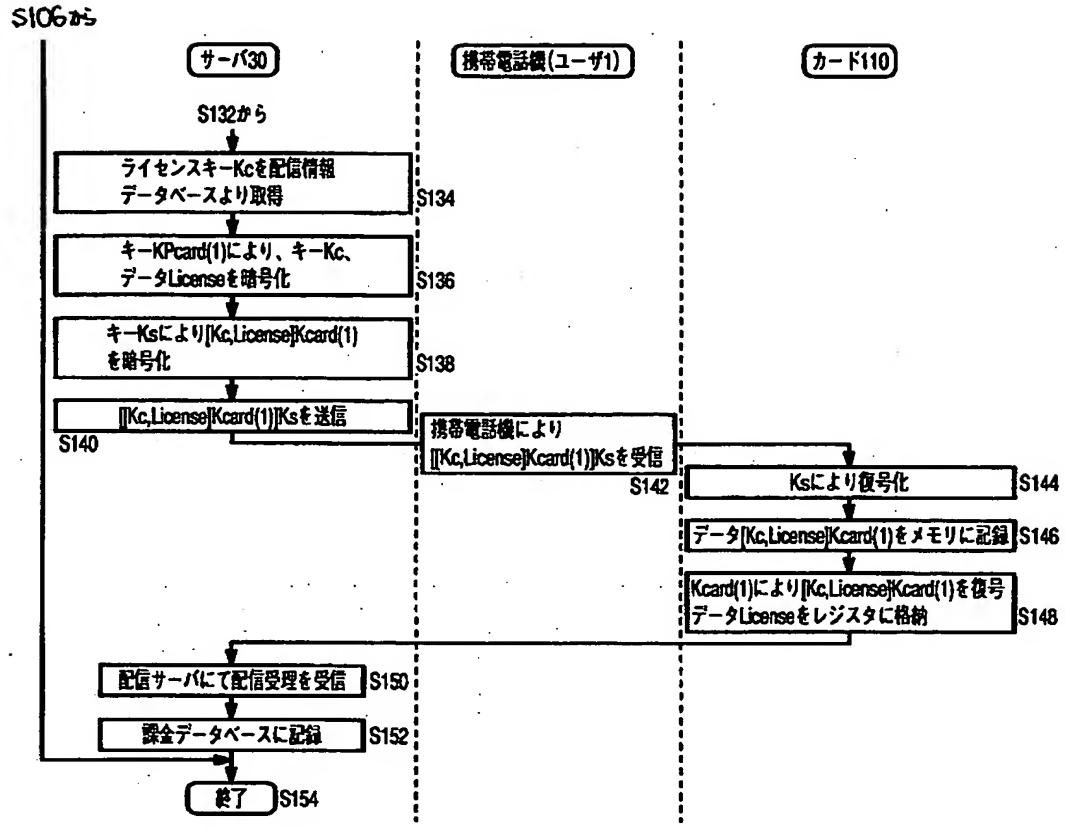
【図５】


110
コントローラ
1420
メモリ
1412
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
復号
1410
暗号化
1406
復号
1404
KPmedia(1)保持
1401
Kmedia(1)保持
1402
BS3
BS4
KPcard(n)
Pc
Pa
Pb
1408
KPcard(1)保持
1405
暗号化
1414
復号
1416
Kcard(1)保持
1415
BS5
Kc,License-ID,User-ID
レジスタ
1500
TRM
1202

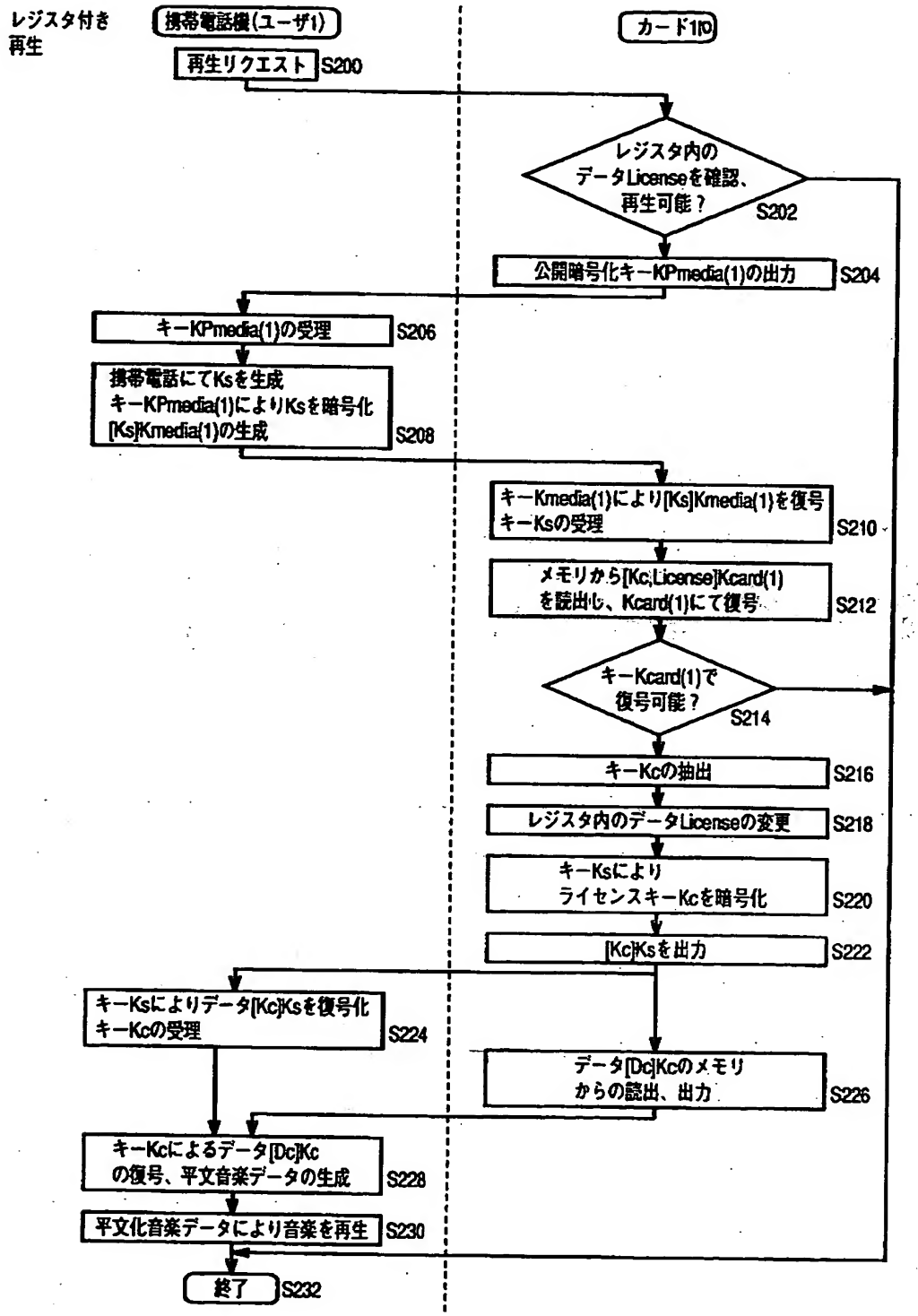
【図６】


配信
サーバ30
携帯電話機(ユーザ1)
カード110
配信リクエスト S100
公開暗号化キーKPmedia(1)を送信 S102
配信リクエストとキーKPmedia(1)を受信 S104
認証サーバにキーKPmedia(1)の確認 S106
配信サーバにてセッションキーKs生成 キーKPmedia(1)にてキーKsを暗号化 データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信 S110
携帯電話機にて[Ks]Kmedia(1)を受信 S112
キーKmedia(1)によりキーKsを復号、抽出 S114
キーKsにより、公開暗号キーKPcard(1)を暗号化 S116
[KPcard(1)]Ksを生成 S118
携帯電話機から配信サーバへ[KPcard(1)]Ksを送信 S120
配信サーバにて[KPcard(1)]Ksを受信 S122
キーKsによりキーKPcard(1)を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信 S128
携帯電話機にてデータ[Dc]Kcを受信 S130
データ[Dc]Kcをメモリに格納 S132
S134へ

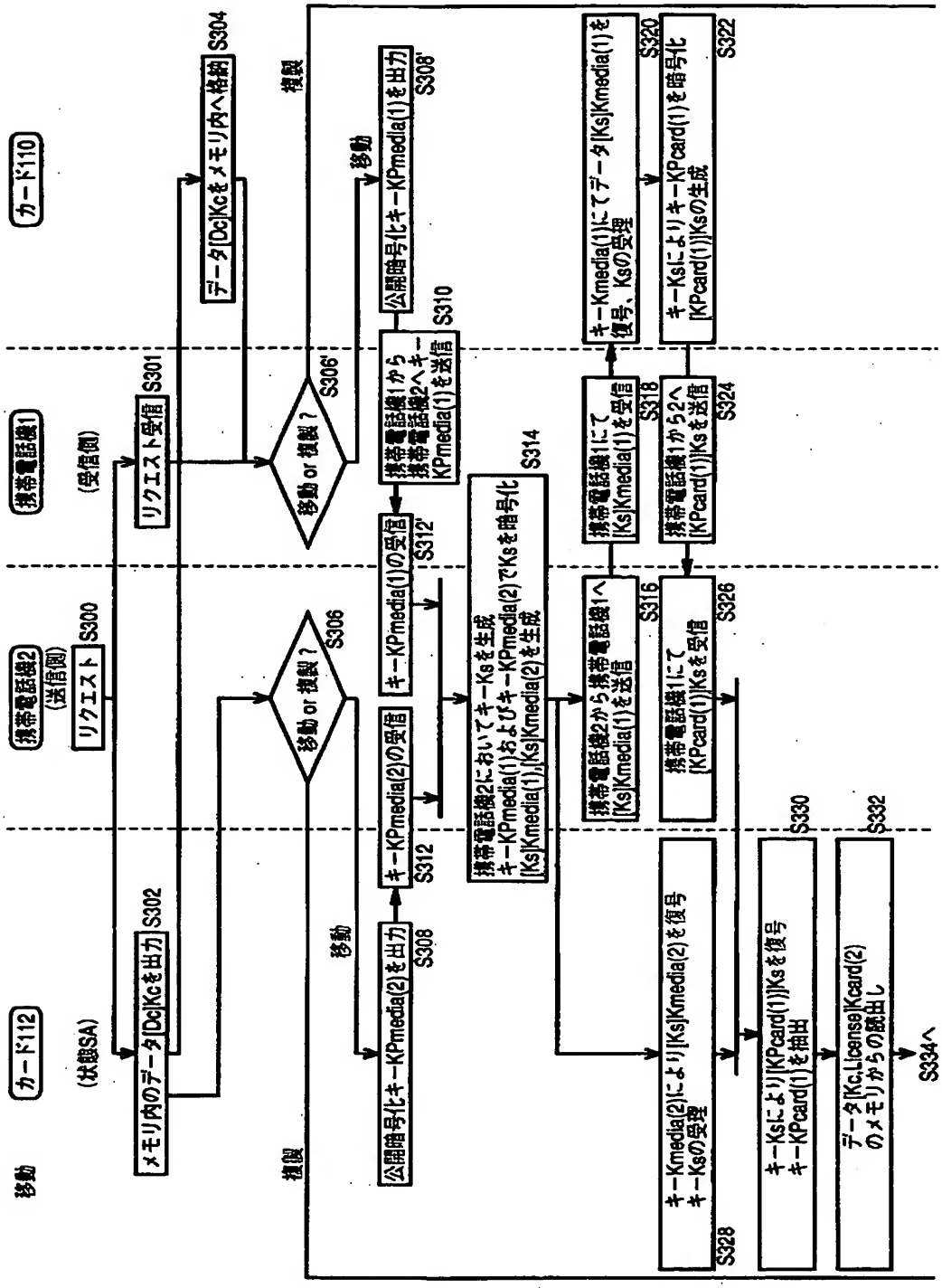
【図７】


S106から
サーバ30
携帯電話機(ユーザ1)
カード110
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKsにより[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ksを送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ksを受信
S142
Ksにより復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

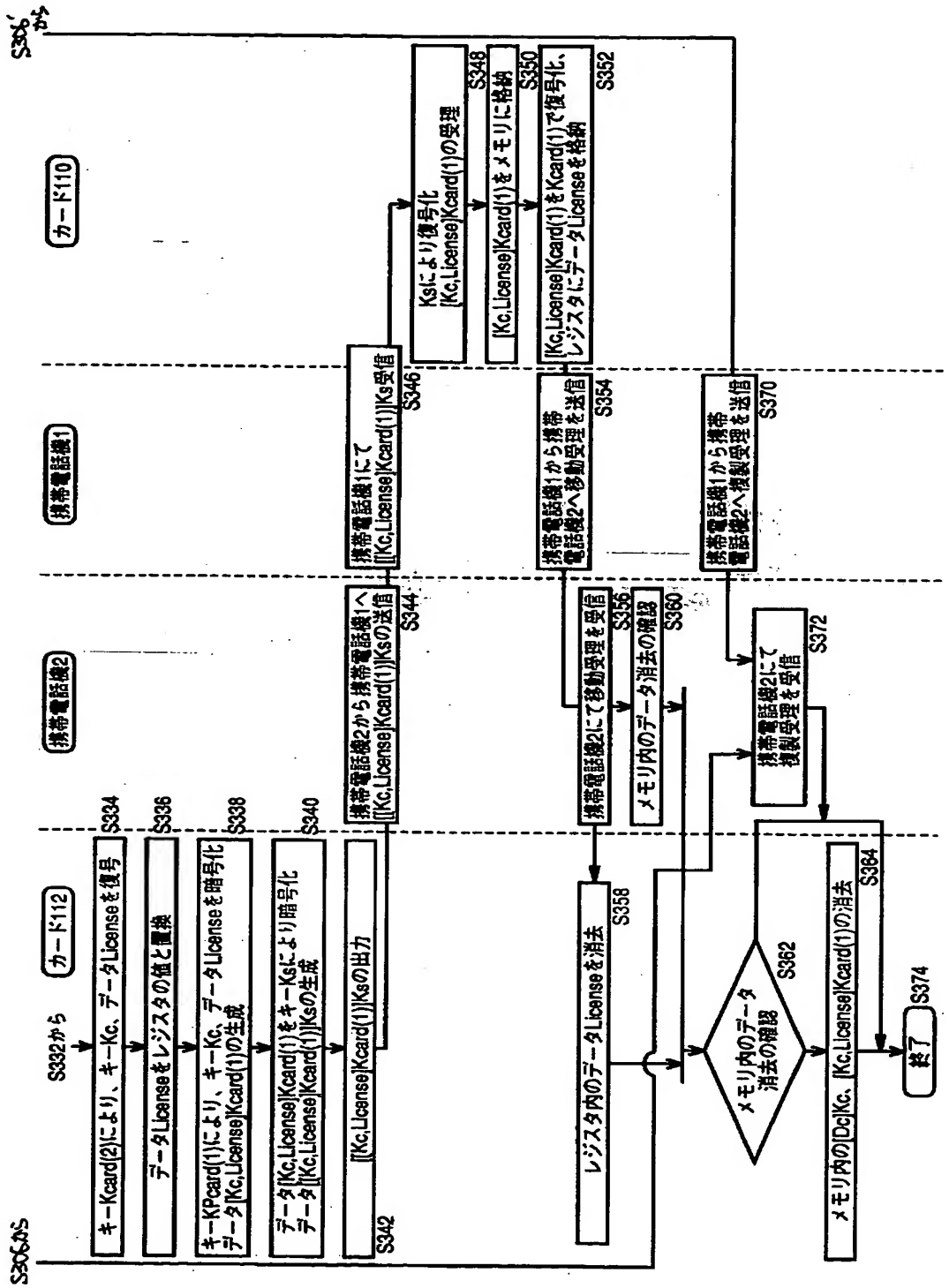
【図８】


レジスタ付き再生
携帯電話機(ユーザ1)
カード1
再生リクエスト S200
レジスタ内のデータLicenseを確認、再生可能？ S202
公開暗号化キーKPmedia(1)の出力 S204
キーKPmedia(1)の受理 S206
携帯電話にてKsを生成 キーKPmedia(1)によりKsを暗号化 [Ks]Kmedia(1)の生成 S208
キーKmedia(1)により[Ks]Kmedia(1)を復号 キーKsの受理 S210
メモリから[Kc,License]Kcard(1)を読出し、Kcard(1)にて復号 S212
キーKcard(1)で復号可能？ S214
キーKcの抽出 S216
レジスタ内のデータLicenseの変更 S218
キーKsによりライセンスキーKcを暗号化 S220
[Kc]Ksを出力 S222
キーKsによりデータ[Kc]Ksを復号化 キーKcの受理 S224
データ[Dc]Kcのメモリからの読出、出力 S226
キーKcによるデータ[Dc]Kcの復号、平文音楽データの生成 S228
平文化音楽データにより音楽を再生 S230
終了 S232

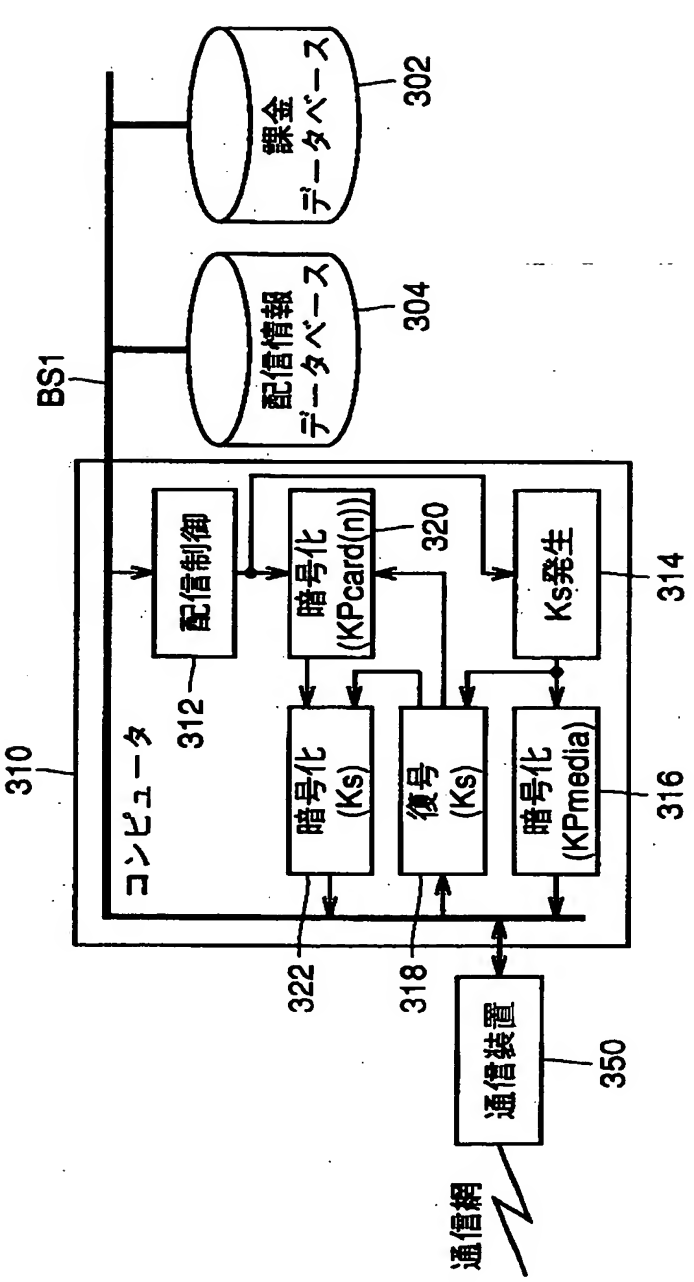
【図９】


移動
カード112
(状態SA)
メモリ内のデータ[Dc]Kcを出力
S302
携帯電話機2
(送信側)
リクエスト
S300
携帯電話機1
(受信側)
リクエスト受信
S301
カード110
データ[Dc]Kcをメモリ内へ格納
S304
移動 or 複製？
S306
移動
公開暗号化キーKPmedia(2)を出力
S308
キーKPmedia(2)の受信
S312
複製
公開暗号化キーKPmedia(1)を出力
S308'
キーKPmedia(1)の受信
S312'
携帯電話機1から携帯電話機2へキーKPmedia(1)を送信
S310
移動 or 複製？
S306'
移動
複製
携帯電話機2においてキーKsを生成
キーKPmedia(1)およびキーKPmedia(2)でKsを暗号化
[Ks]Kmedia(1),[Ks]Kmedia(2)を生成
S314
携帯電話機2から携帯電話機1へ[Ks]Kmedia(1)を送信
S316
携帯電話機1にて[Ks]Kmedia(1)を受信
S318
キーKmedia(1)にてデータ[Ks]Kmedia(1)を復号、Ksの受理
S320
携帯電話機1から2へ[KPcard(1)]Ksを送信
S324
キーKsによりキーKPcard(1)を暗号化[KPcard(1)]Ksの生成
S322
携帯電話機1にて[KPcard(1)]Ksを受信
S326
キーKmedia(2)により[Ks]Kmedia(2)を復号
キーKsの受理
S328
キーKsにより[KPcard(1)]Ksを復号
キーKPcard(1)を抽出
S330
データ[Kc,License]Kcard(2)のメモリからの読出し
S332
S334へ

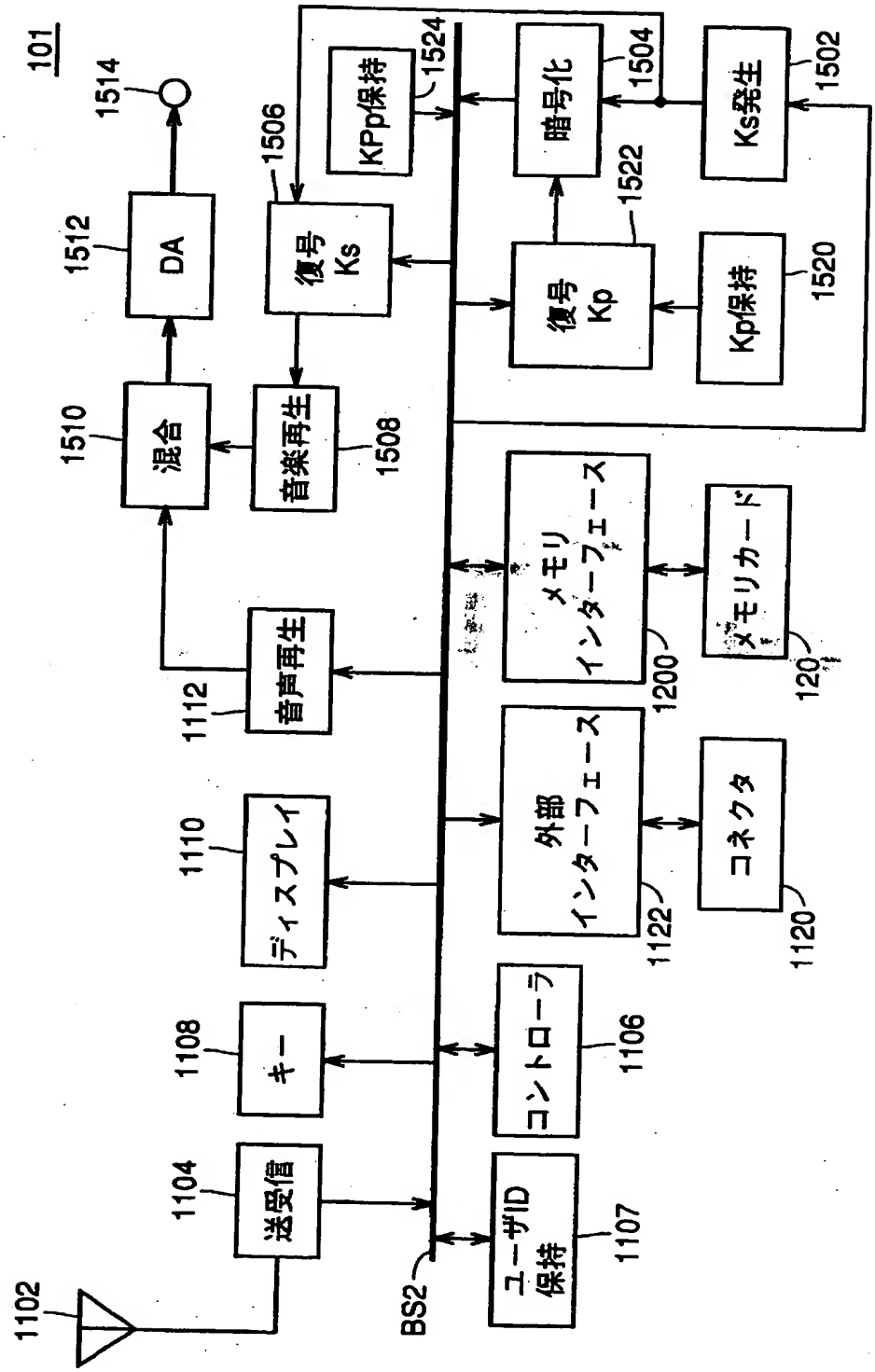
【図１０】


S305から
カード110
携帯電話機1
携帯電話機2
カード112
S332から
キーKcard(2)により、キーKc、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S336
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ[Kc,License]Kcard(1)の生成
S338
データ[Kc,License]Kcard(1)をキーKsにより暗号化
データ[[Kc,License]Kcard(1)]Ksの生成
S340
[[Kc,License]Kcard(1)]Ksの出力
S342
携帯電話機2から携帯電話機1へ
[[Kc,License]Kcard(1)]Ksの送信
S344
携帯電話機1にて
[[Kc,License]Kcard(1)]Ks受信
S346
Ksにより復号化
[Kc,License]Kcard(1)の受理
S348
[Kc,License]Kcard(1)をメモリに格納
S350
[Kc,License]Kcard(1)をKcard(1)で復号化、
レジスタにデータLicenseを格納
S352
携帯電話機1から携帯
電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯
電話機2へ複製受理を送信
S370
携帯電話機2にて
複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ
消去の確認
S362
メモリ内の[Dc]Kc、[Kc,License]Kcard(1)の消去
S364
終了
S374
S305から

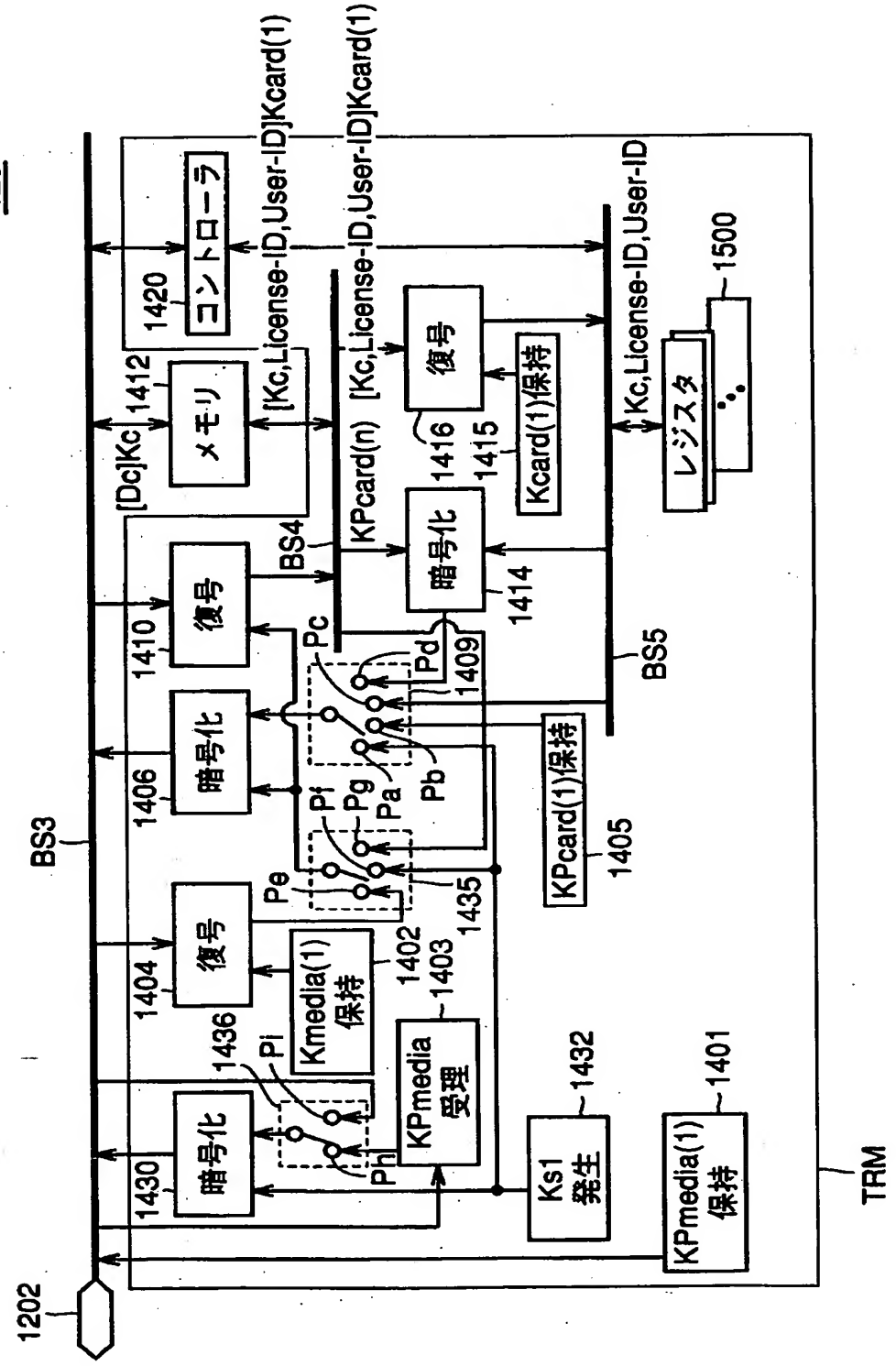
【図１１】


31
課金データベース
302
配信情報データベース
304
BS1
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
コンピュータ
310
暗号化(Ks)
復号(Ks)
暗号化(KPmedia)
316
322
318
通信装置
350
通信網

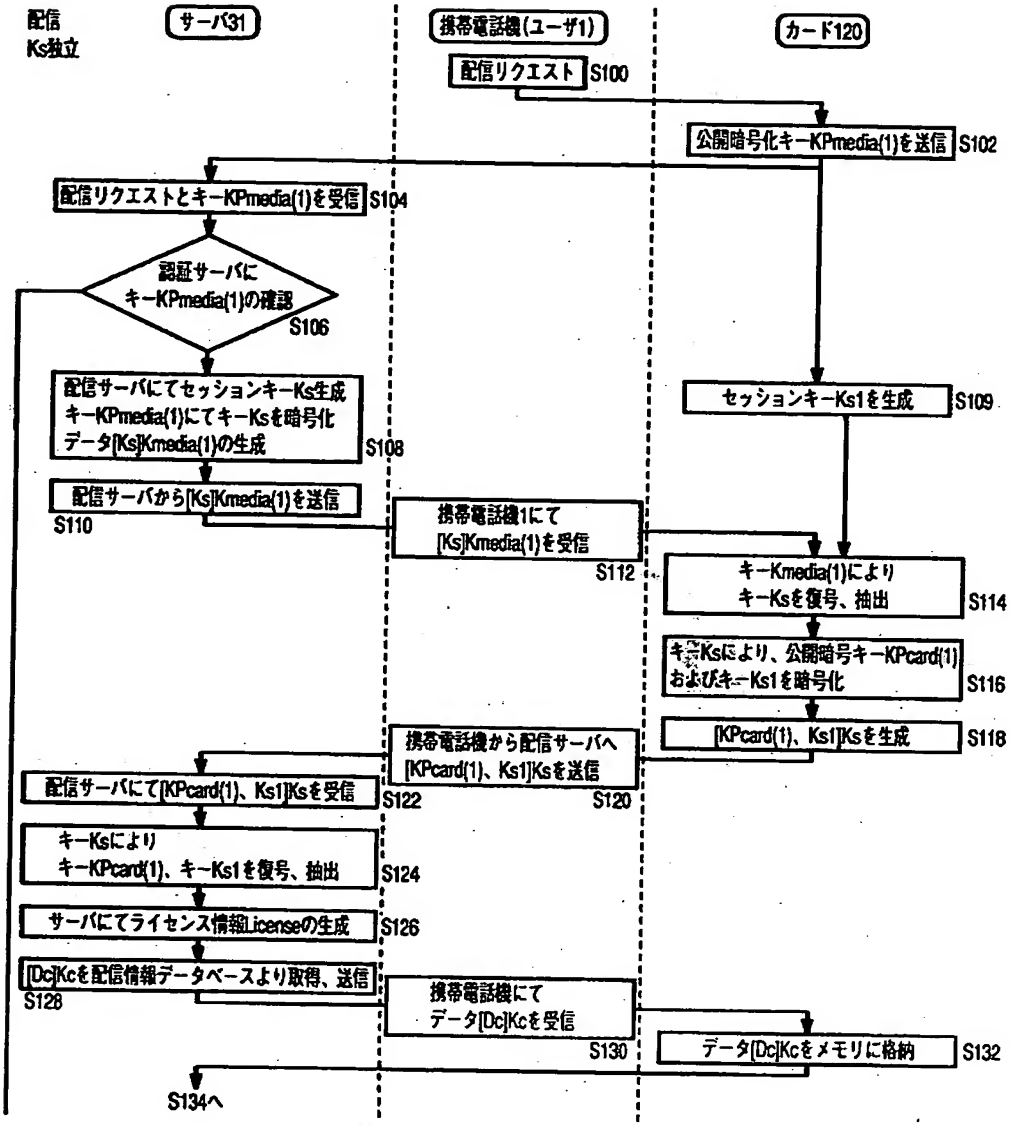
【図１２】


101
1514
1512
DA
1510
混合
1112
音声再生
1110
ディスプレイ
1108
キー
1104
送受信
1102
BS2
ユーザID保持
1107
コントローラ
1106
1506
復号Ks
1508
音楽再生
KPp保持
1524
暗号化
1504
Ks発生
1502
1522
復号Kp
Kp保持
1520
メモリインターフェース
1200
メモリカード
120
外部インターフェース
1122
コネクタ
1120

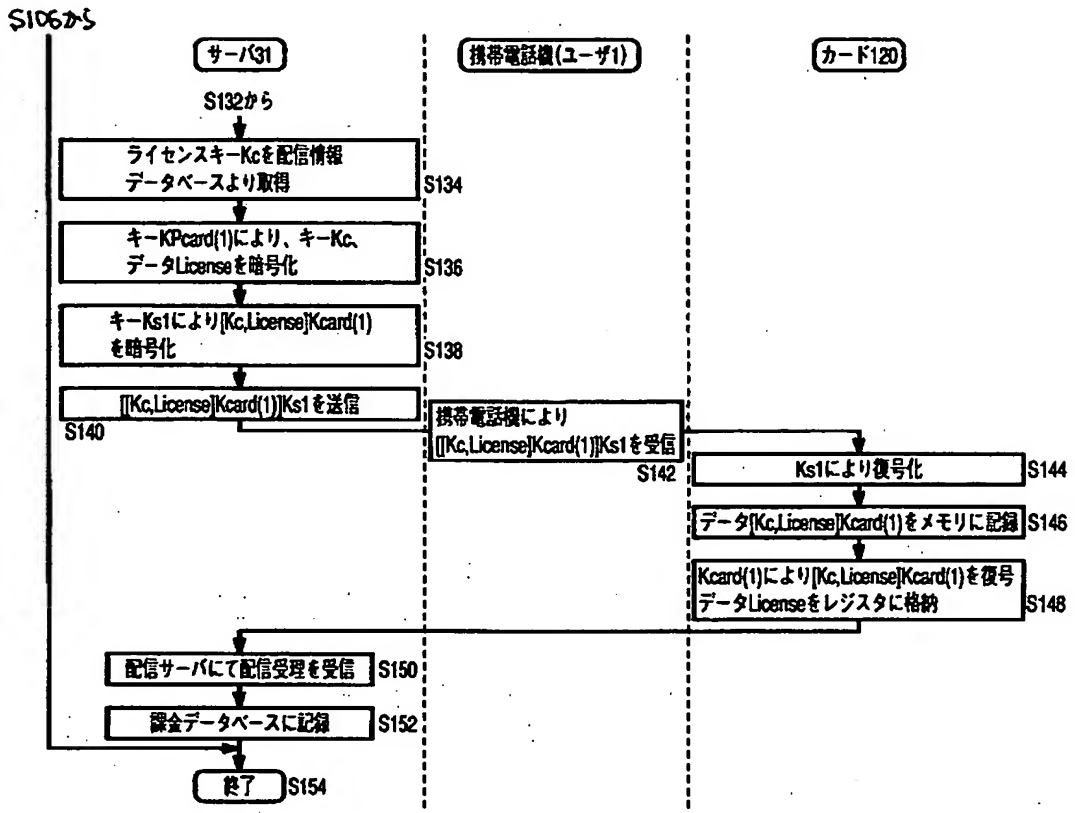
【図１３】


120
コントローラ
1420
メモリ
1412
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
Kc,License-ID,User-ID
1500
レジスタ
復号
1410
暗号化
1406
復号
1404
暗号化
1430
BS3
BS4
BS5
KPcard(n)
暗号化
1414
復号
1416
Kcard(1)保持
1415
KPcard(1)保持
1405
Kmedia(1)
保持
1402
KPmedia
受理
1403
Ks1
発生
1432
KPmedia(1)
保持
1401
TRM
1202
1409
1435
1436
Pa
Pb
Pc
Pd
Pe
Pf
Pg
Ph
Pi

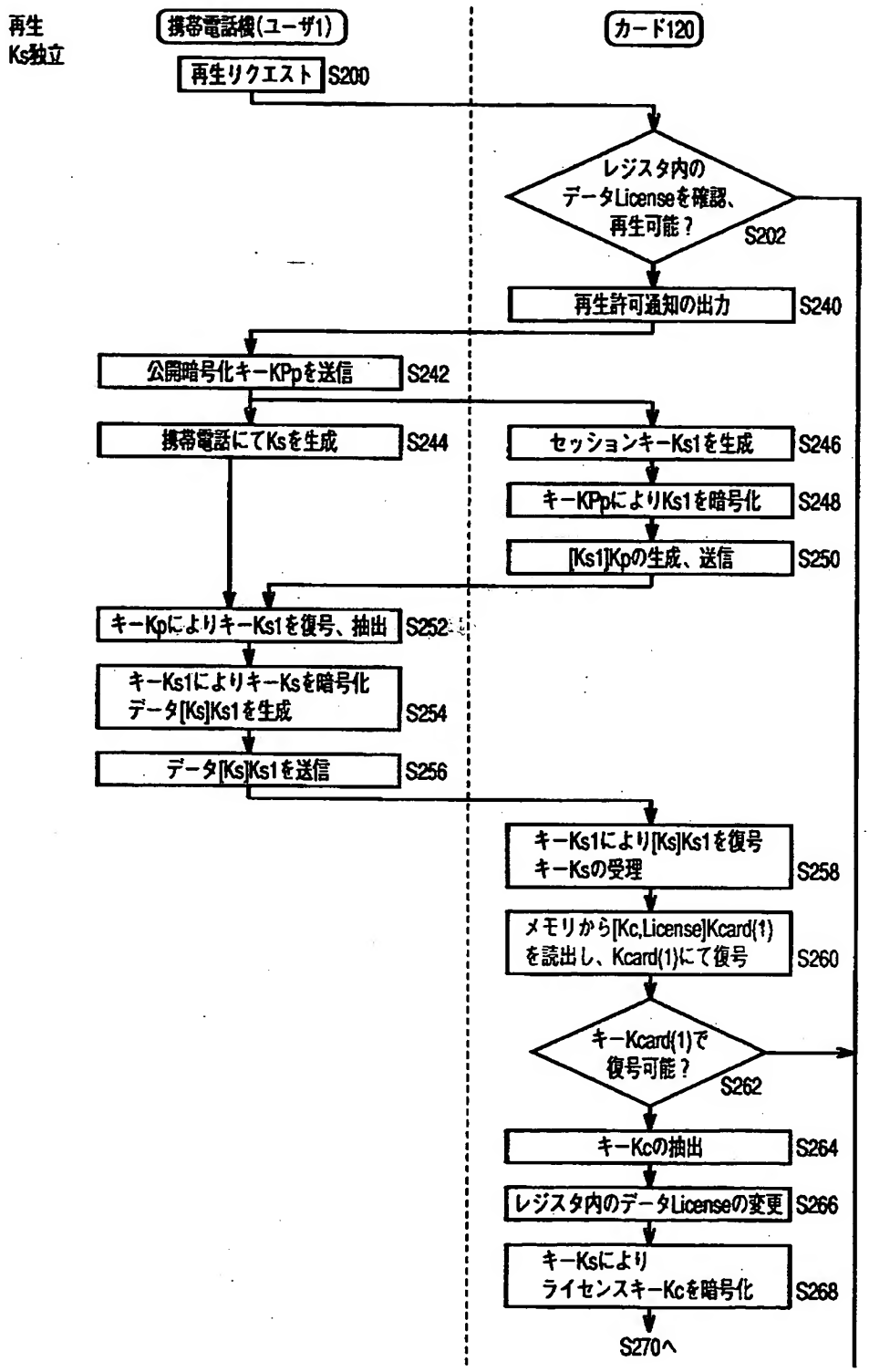
【図１４】


配信
Ks独立
サーバ31
携帯電話機(ユーザ1)
カード120
配信リクエスト S100
公開暗号化キーKPmedia(1)を送信 S102
配信リクエストとキーKPmedia(1)を受信 S104
認証サーバに
キーKPmedia(1)の確認
S106
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
セッションキーKs1を生成 S109
配信サーバから[Ks]Kmedia(1)を送信
S110
携帯電話機1にて
[Ks]Kmedia(1)を受信
S112
キーKmedia(1)により
キーKsを復号、抽出 S114
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ
[KPcard(1)、Ks1]Ksを送信
S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信
S122
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信
S128
携帯電話機にて
データ[Dc]Kcを受信
S130
データ[Dc]Kcをメモリに格納 S132
S134へ

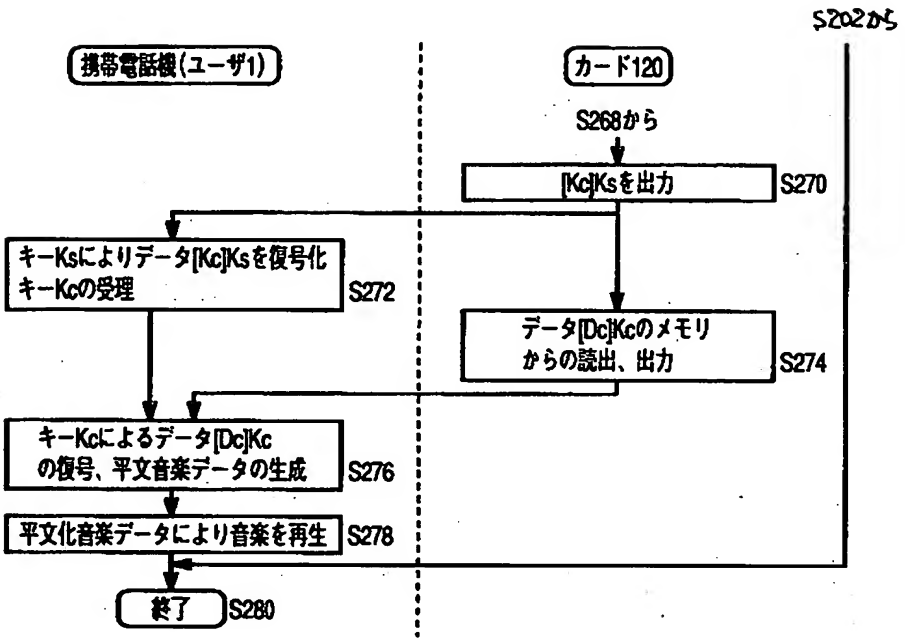
【図１５】


S106から
サーバ31
携帯電話機(ユーザ1)
カード120
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKs1により[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ks1を送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

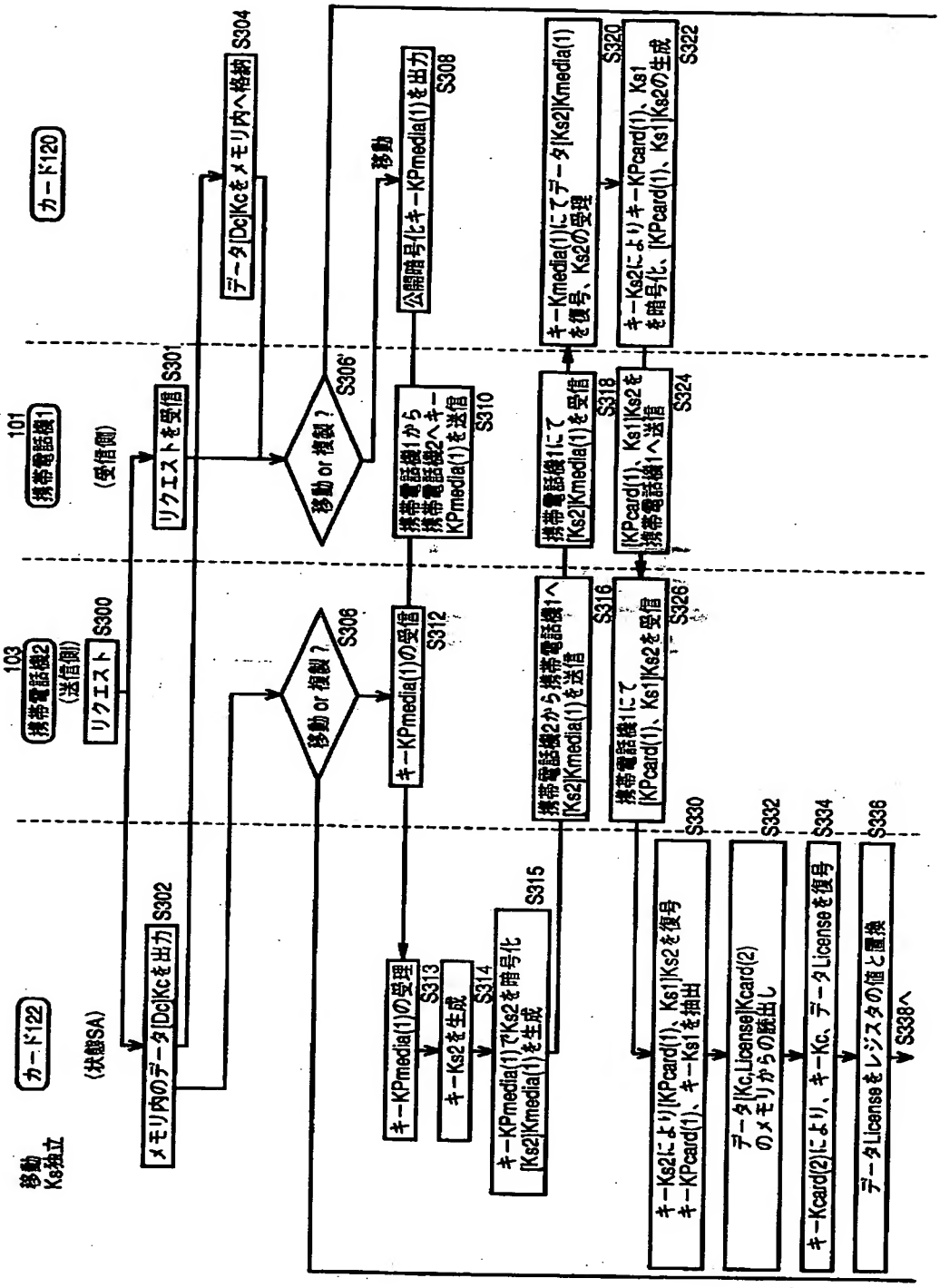
【図１６】


再生
Ks独立
携帯電話機(ユーザ1)
カード120
再生リクエスト S200
レジスタ内のデータLicenseを確認、再生可能？ S202
再生許可通知の出力 S240
公開暗号化キーKPpを送信 S242
携帯電話にてKsを生成 S244
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]Kpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
キーKs1によりキーKsを暗号化データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号キーKsの受理 S258
メモリから[Kc,License]Kcard(1)を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
キーKcの抽出 S264
レジスタ内のデータLicenseの変更 S266
キーKsによりライセンスキーKcを暗号化 S268
S270へ

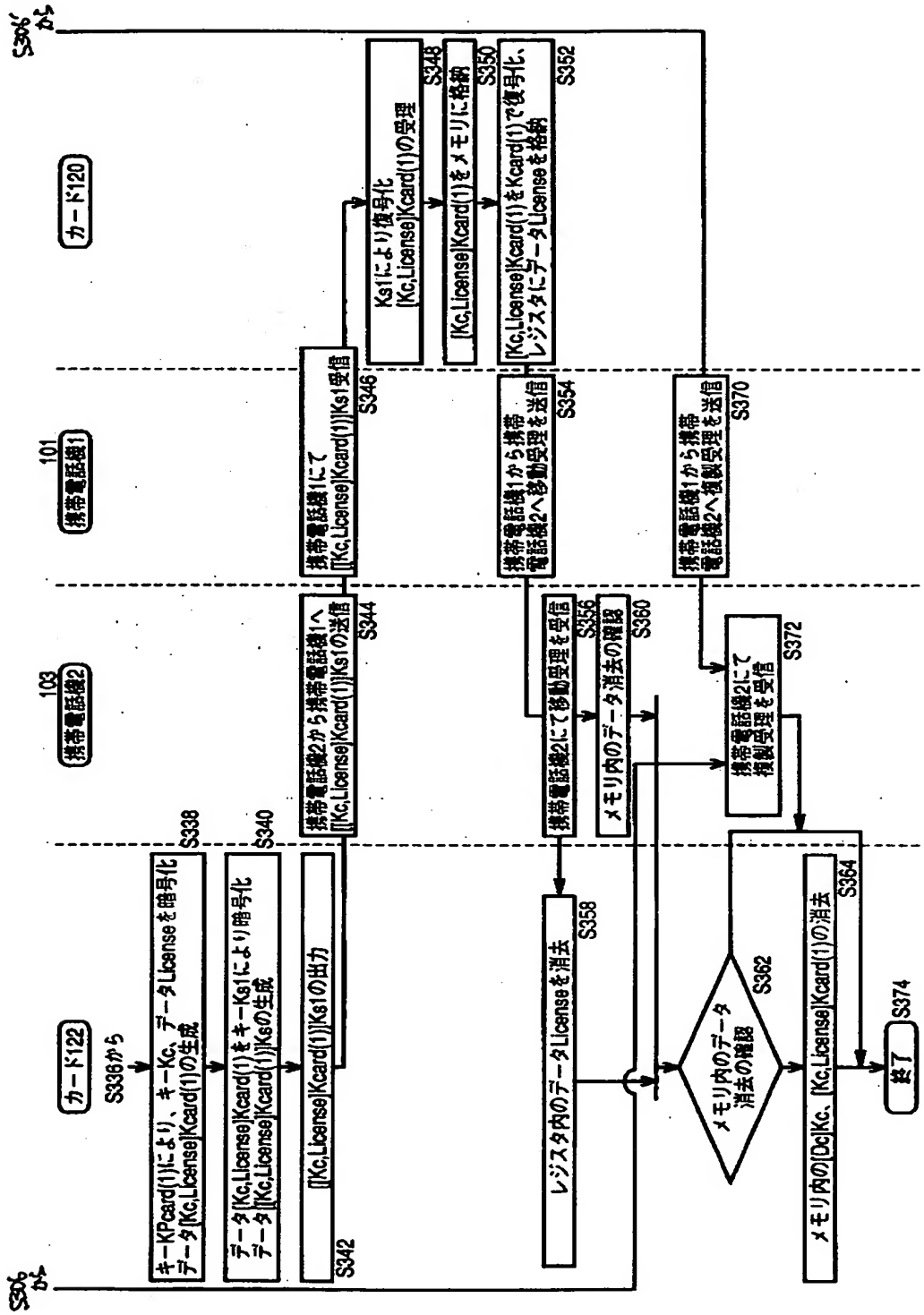
【図１７】


S202から
携帯電話機(ユーザ1)
カード120
S268から
[Kc]Ksを出力
S270
キーKsによりデータ[Kc]Ksを復号化
キーKcの受理
S272
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kc
の復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

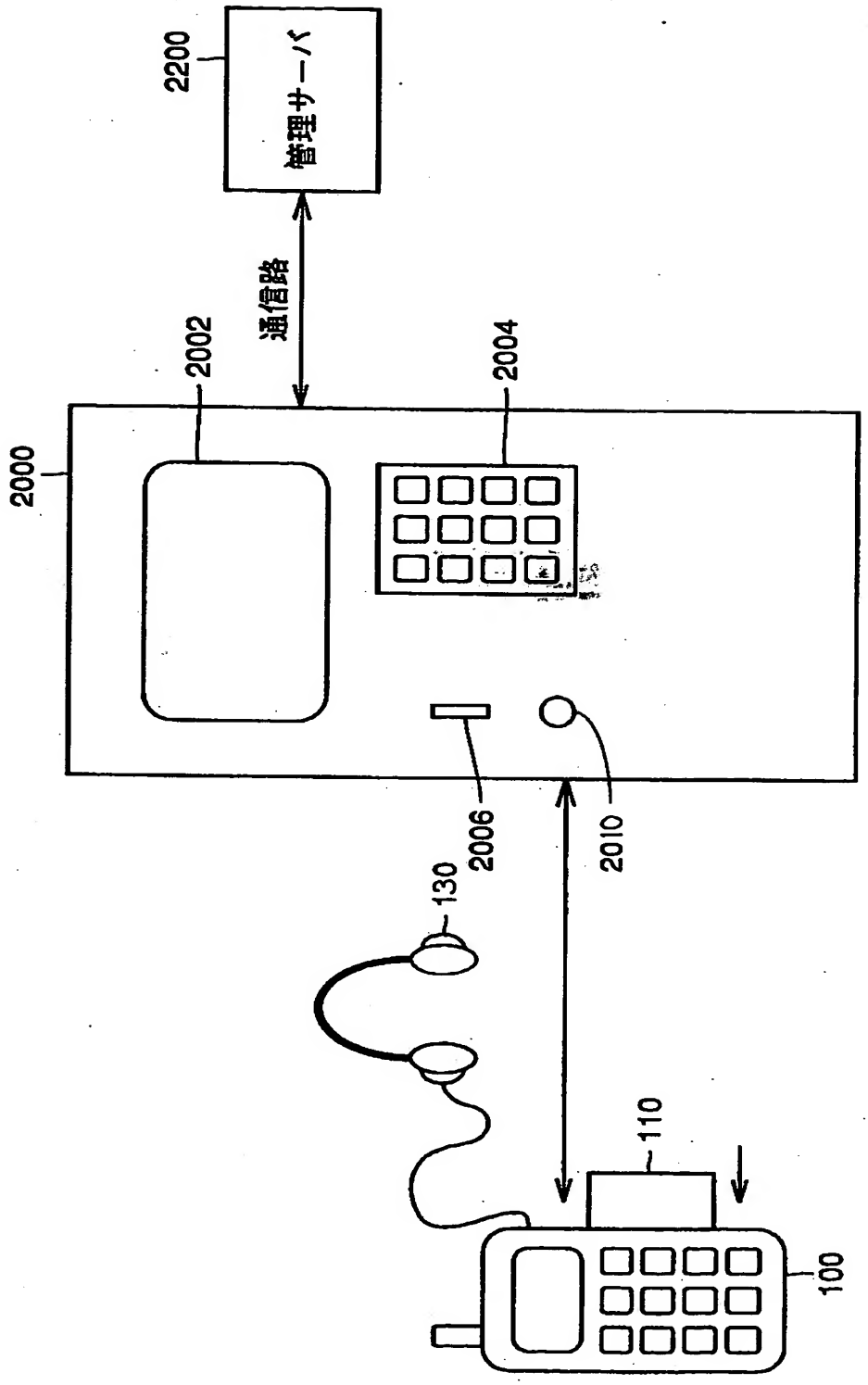
【図１８】


移動
Ks独立
カード122
(状態SA)
メモリ内のデータ[Dc]Kcを出力
S302
103
携帯電話機2
(送信側)
リクエスト
S300
リクエストを受信
S301
101
携帯電話機1
(受信側)
カード120
データ[Dc]Kcをメモリ内へ格納
S304
移動 or 複製？
S306
移動
公開暗号化キーKPmedia(1)を出力
S308
携帯電話機1から携帯電話機2へキーKPmedia(1)を送信
S310
キーKPmedia(1)の受理
S312
キーKPmedia(1)の受理
S313
キーKs2を生成
S314
キーKPmedia(1)でKs2を暗号化[Ks2]Kmedia(1)を生成
S315
携帯電話機2から携帯電話機1へ[Ks2]Kmedia(1)を送信
S316
携帯電話機1にて[Ks2]Kmedia(1)を受信
S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を復号、Ks2の受理
S320
キーKs2によりキーKPcard(1)、Ks1を暗号化、[KPcard(1)、Ks1]Ks2の生成
S322
[KPcard(1)、Ks1]Ks2を携帯電話機1へ送信
S324
携帯電話機1にて[KPcard(1)、Ks1]Ks2を受信
S326
キーKs2により[KPcard(1)、Ks1]Ks2を復号
キーKPcard(1)、キーKs1を抽出
S330
データ[Kc,License]Kcard(2)のメモリからの読出し
S332
キーKcard(2)により、キーKc、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S336
S338へ

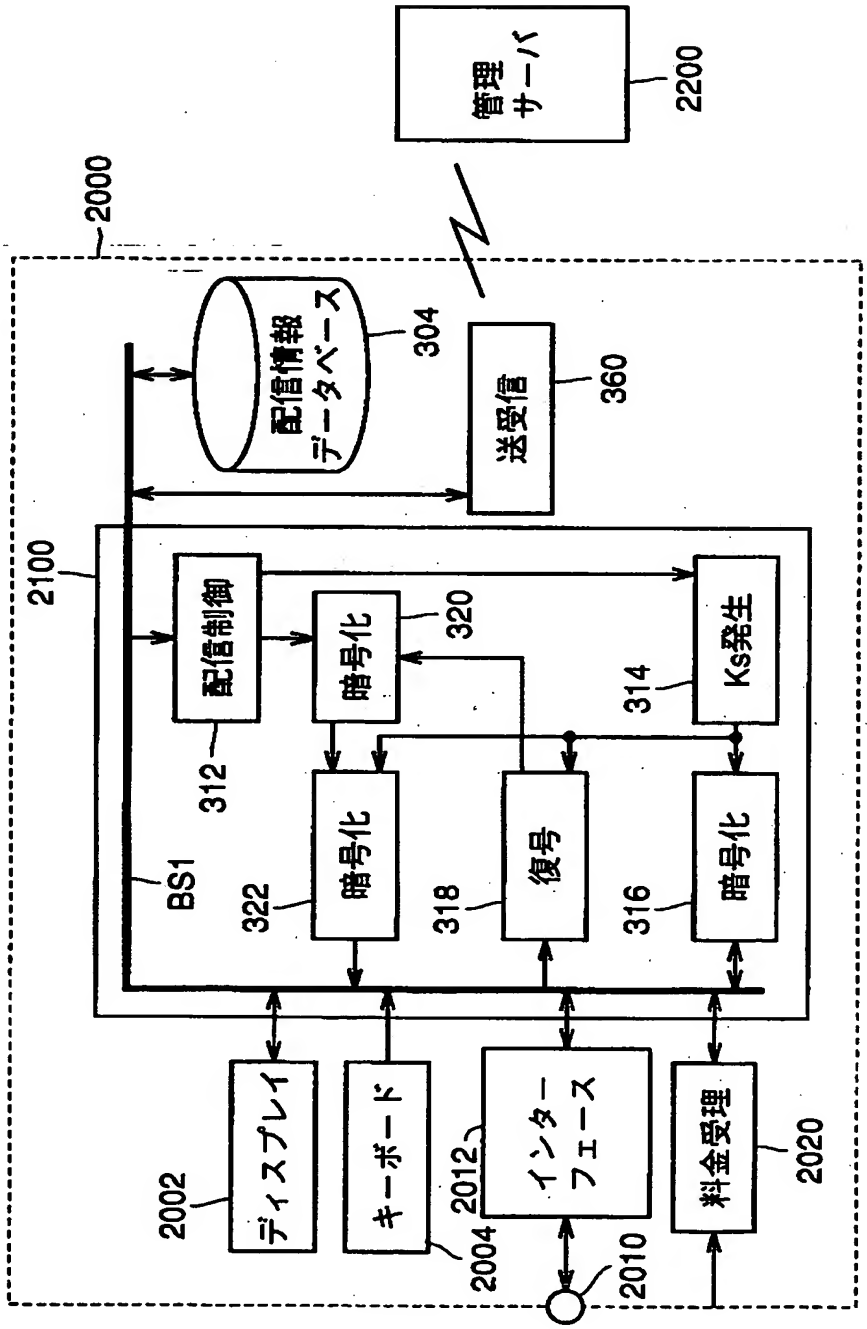
【図１９】


S306から
カード120
101
携帯電話機1
103
携帯電話機2
カード122
S336から
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ[Kc,License]Kcard(1)の生成
S338
データ[Kc,License]Kcard(1)をキーKs1により暗号化
データ[[Kc,License]Kcard(1)]Ksの生成
S340
[[Kc,License]Kcard(1)]Ks1の出力
S342
携帯電話機2から携帯電話機1へ
[[Kc,License]Kcard(1)]Ks1の送信
S344
携帯電話機1にて
[[Kc,License]Kcard(1)]Ks1受信
S346
Ks1により復号化
[Kc,License]Kcard(1)の受理
S348
[Kc,License]Kcard(1)をメモリに格納
S350
[Kc,License]Kcard(1)をKcard(1)で復号化、
レジスタにデータLicenseを格納
S352
携帯電話機1から携帯
電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯
電話機2へ複製受理を送信
S370
携帯電話機2にて
複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ
消去の確認
S362
メモリ内の[Dc]Kc、[Kc,License]Kcard(1)の消去
S364
終了
S374

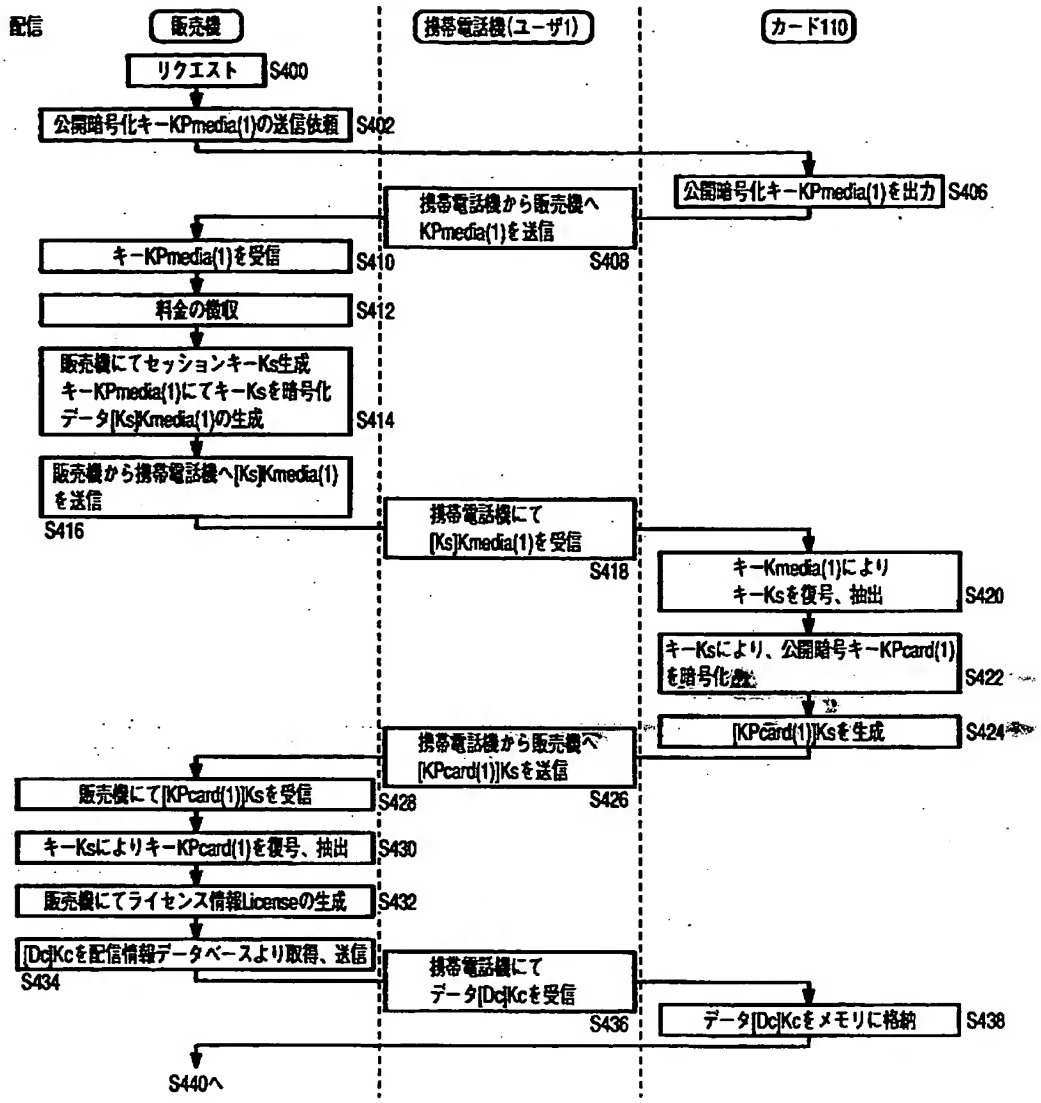
【図２０】



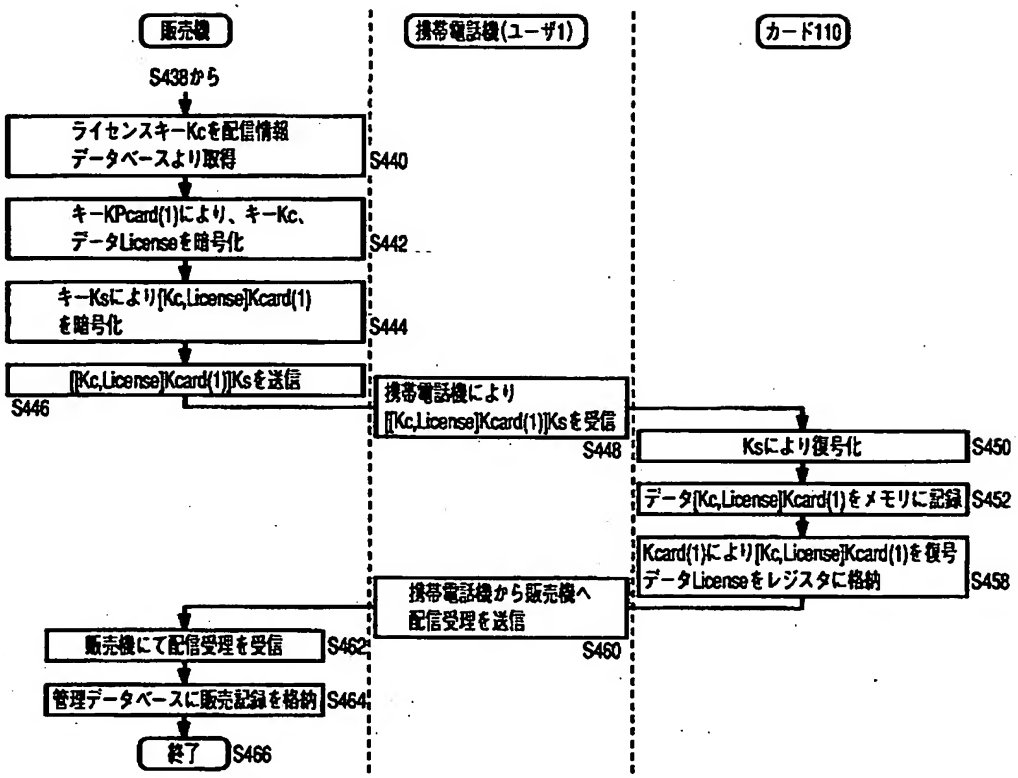
【図２１】


管理サーバ
2200
2000
配信情報データベース
304
送受信
360
2100
配信制御
暗号化
320
Ks発生
314
312
暗号化
復号
暗号化
BS1
322
318
316
ディスプレイ
キーボード
インターフェース
料金受理
2020
2002
2012
2004
2010

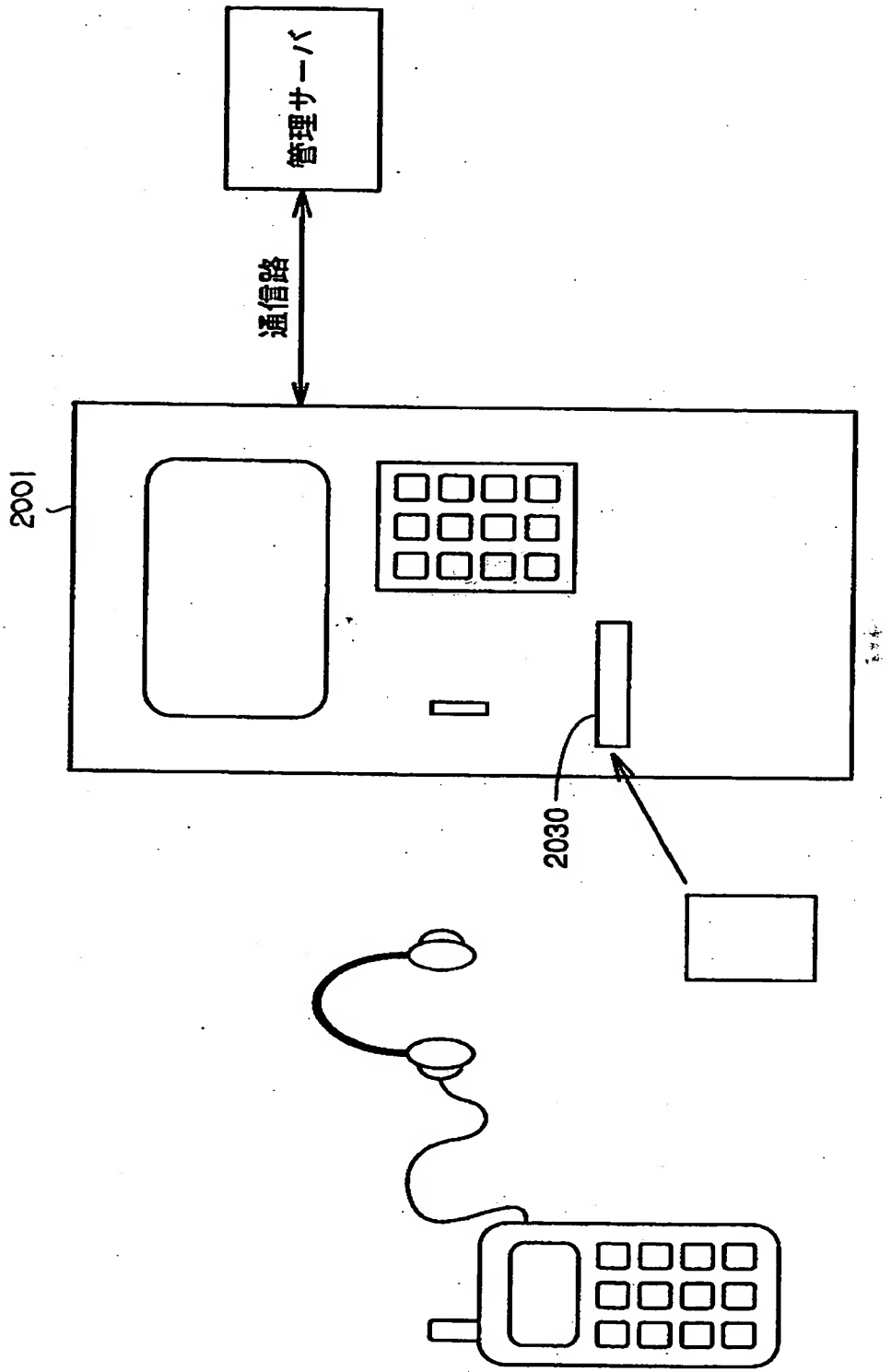
【図２２】


配信
販売機
携帯電話機(ユーザ1)
カード110
リクエスト S400
公開暗号化キーKPmedia(1)の送信依頼 S402
公開暗号化キーKPmedia(1)を出力 S406
携帯電話機から販売機へ KPmedia(1)を送信 S408
キーKPmedia(1)を受信 S410
料金の徴収 S412
販売機にてセッションキーKs生成 キーKPmedia(1)にてキーKsを暗号化 データ[Ks]Kmedia(1)の生成 S414
販売機から携帯電話機へ[Ks]Kmedia(1)を送信 S416
携帯電話機にて [Ks]Kmedia(1)を受信 S418
キーKmedia(1)により キーKsを復号、抽出 S420
キーKsにより、公開暗号キーKPcard(1)を暗号化 S422
[KPcard(1)]Ksを生成 S424
携帯電話機から販売機へ [KPcard(1)]Ksを送信 S426
販売機にて[KPcard(1)]Ksを受信 S428
キーKsによりキーKPcard(1)を復号、抽出 S430
販売機にてライセンス情報Licenseの生成 S432
[Dc]Kcを配信情報データベースより取得、送信 S434
携帯電話機にて データ[Dc]Kcを受信 S436
データ[Dc]Kcをメモリに格納 S438
S440へ

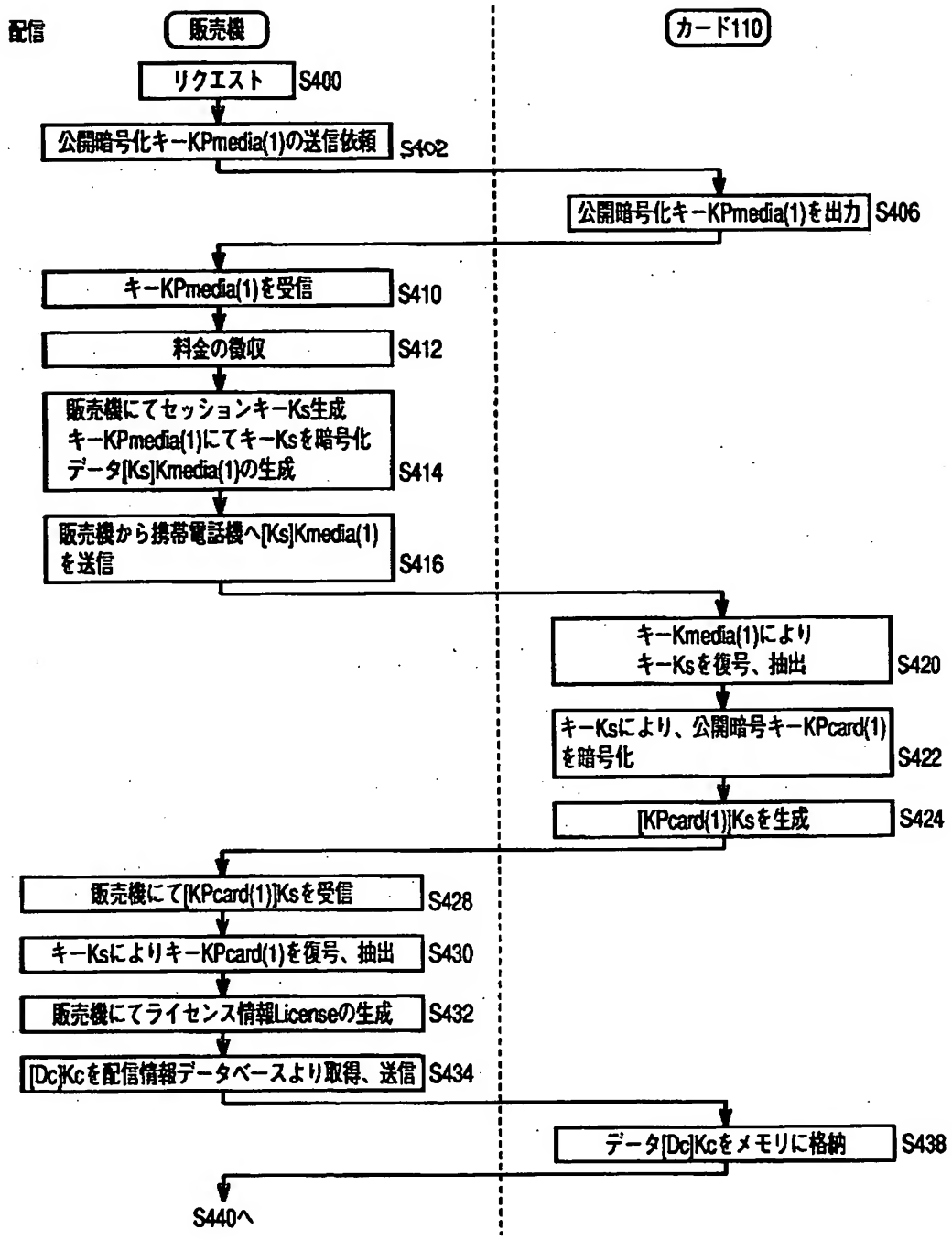
【図２３】


販売機
携帯電話機(ユーザ1)
カード110
S438から
ライセンスキーKcを配信情報データベースより取得
S440
キーKPcard(1)により、キーKc、データLicenseを暗号化
S442
キーKsにより[Kc,License]Kcard(1)を暗号化
S444
[Kc,License]Kcard(1)]Ksを送信
S446
携帯電話機により[[Kc,License]Kcard(1)]Ksを受信
S448
Ksにより復号化
S450
データ[Kc,License]Kcard(1)をメモリに記録
S452
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S458
携帯電話機から販売機へ配信受理を送信
S460
販売機にて配信受理を受信
S462
管理データベースに販売記録を格納
S464
終了
S466

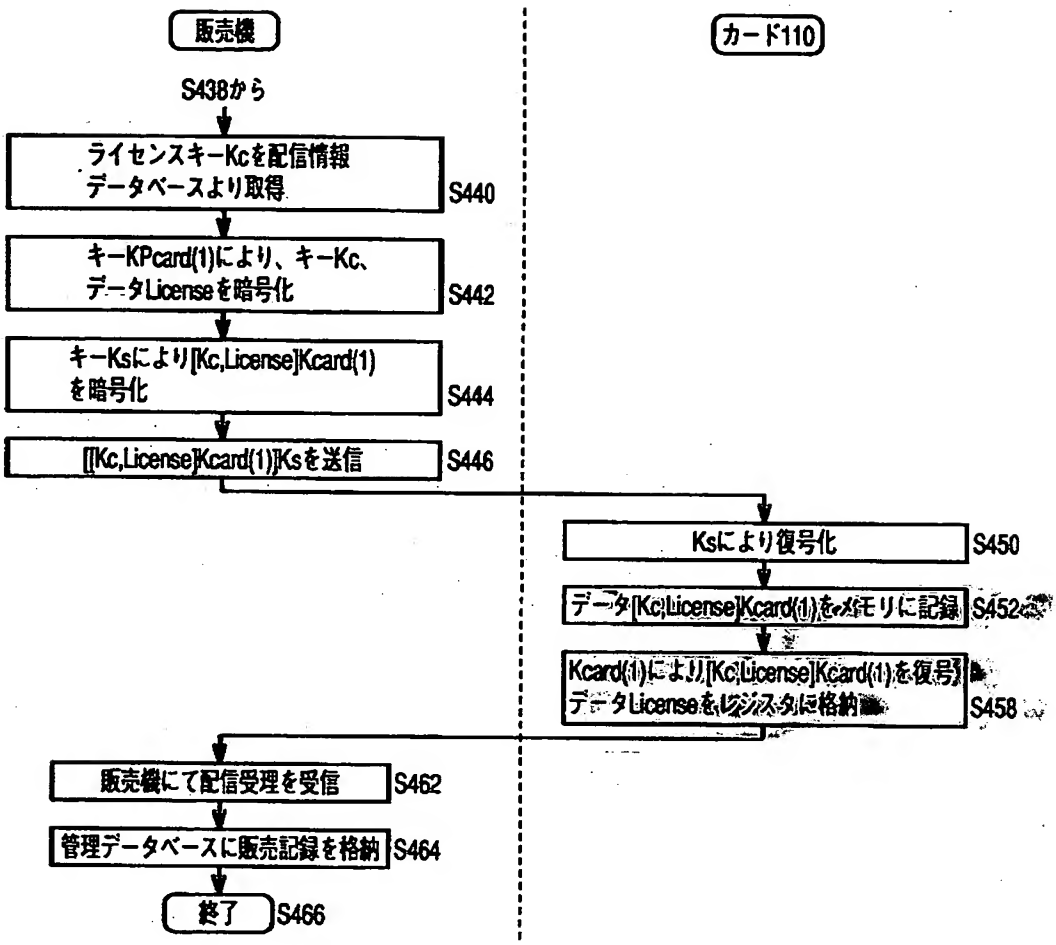
【図２４】



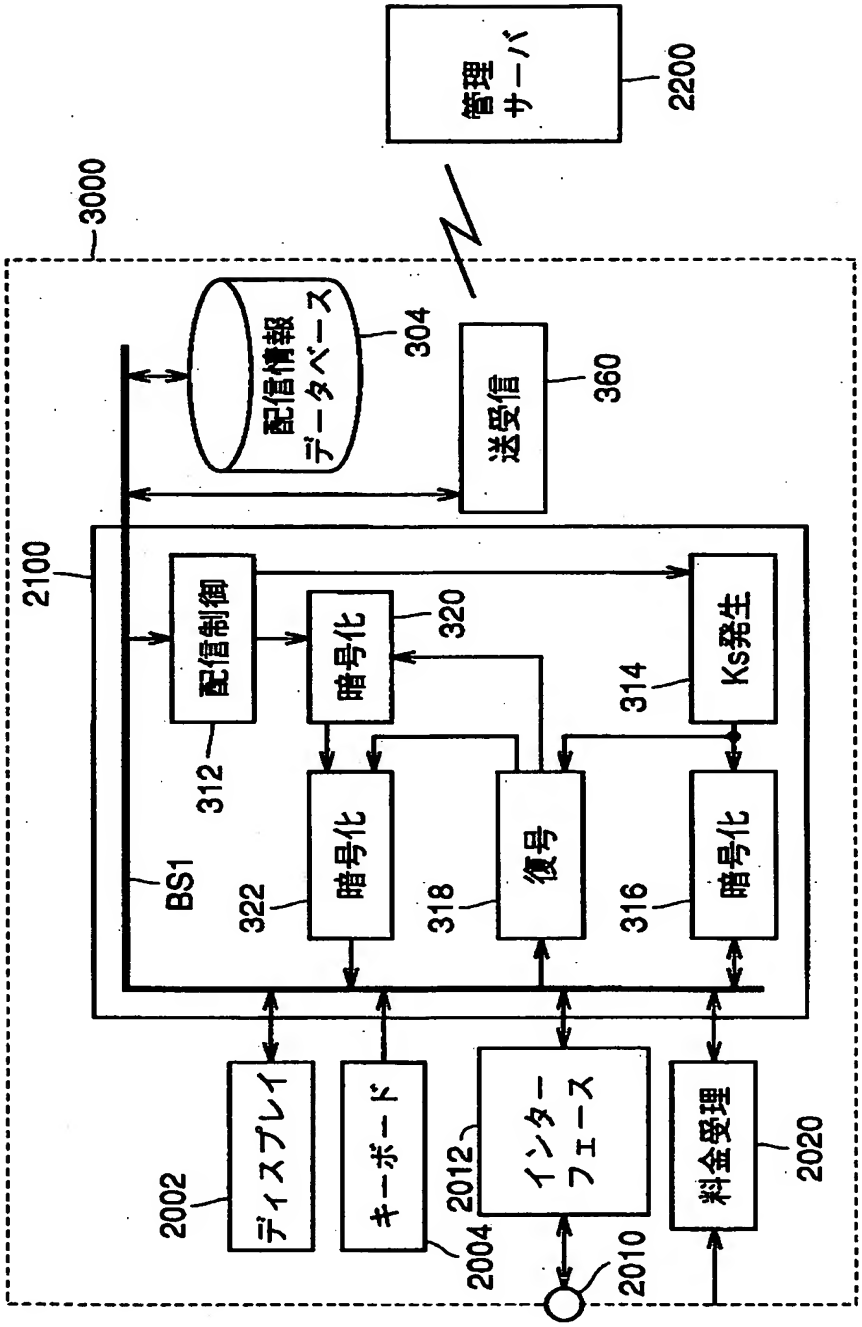
【図２５】


配信
販売機
カード110
リクエスト
S400
公開暗号化キーKPmedia(1)の送信依頼
S402
公開暗号化キーKPmedia(1)を出力
S406
キーKPmedia(1)を受信
S410
料金の徴収
S412
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S414
販売機から携帯電話機へ[Ks]Kmedia(1)
を送信
S416
キーKmedia(1)により
キーKsを復号、抽出
S420
キーKsにより、公開暗号キーKPcard(1)
を暗号化
S422
[KPcard(1)]Ksを生成
S424
販売機にて[KPcard(1)]Ksを受信
S428
キーKsによりキーKPcard(1)を復号、抽出
S430
販売機にてライセンス情報Licenseの生成
S432
[Dc]Kcを配信情報データベースより取得、送信
S434
データ[Dc]Kcをメモリに格納
S438
S440へ

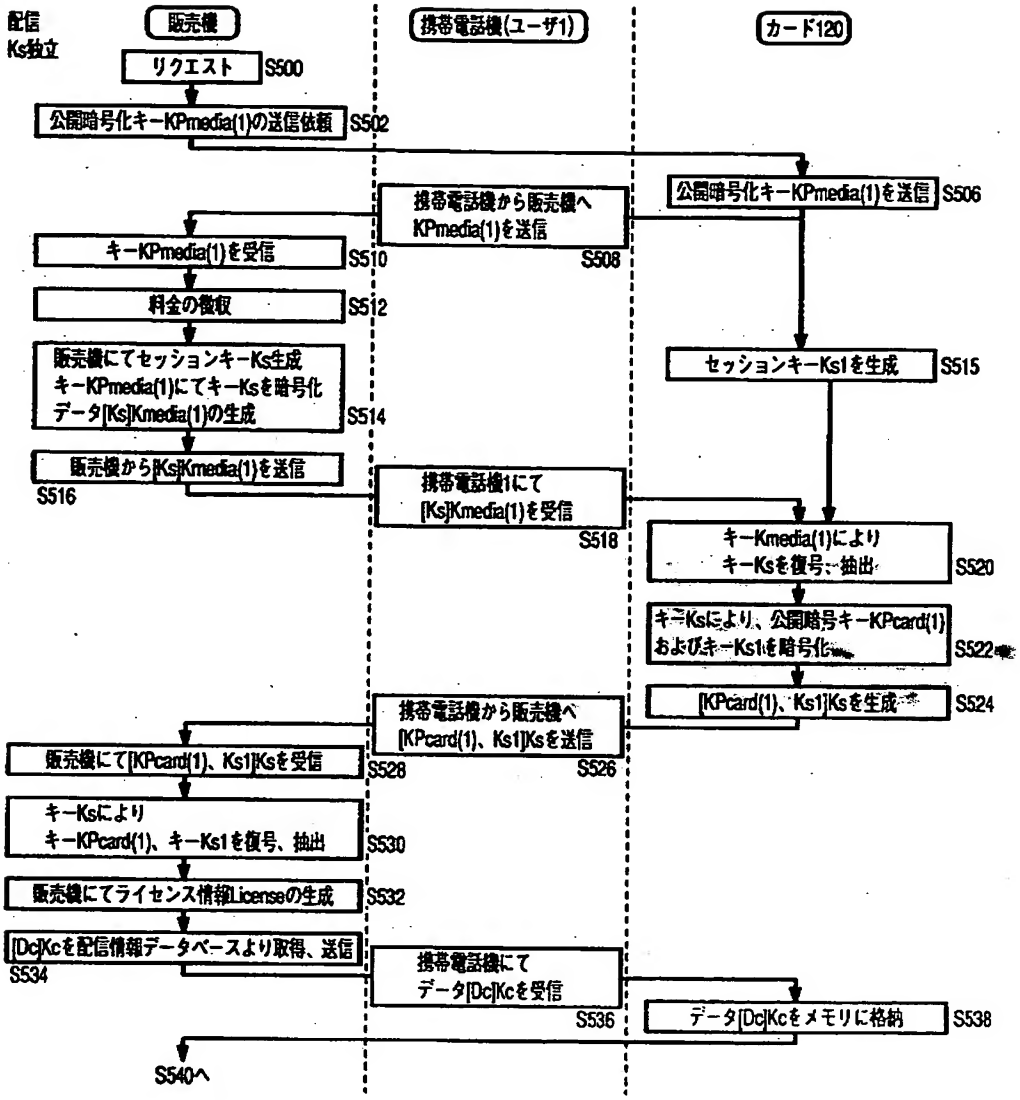
【図２６】


販売機
カード110
S438から
ライセンスキーKcを配信情報データベースより取得
S440
キーKPcard(1)により、キーKc、データLicenseを暗号化
S442
キーKsにより[Kc,License]Kcard(1)を暗号化
S444
[[Kc,License]Kcard(1)]Ksを送信
S446
Ksにより復号化
S450
データ[Kc,License]Kcard(1)をメモリに記録
S452
Kcard(1)により[Kc,License]Kcard(1)を復号
データLicenseをレジスタに格納
S458
販売機にて配信受理を受信
S462
管理データベースに販売記録を格納
S464
終了
S466

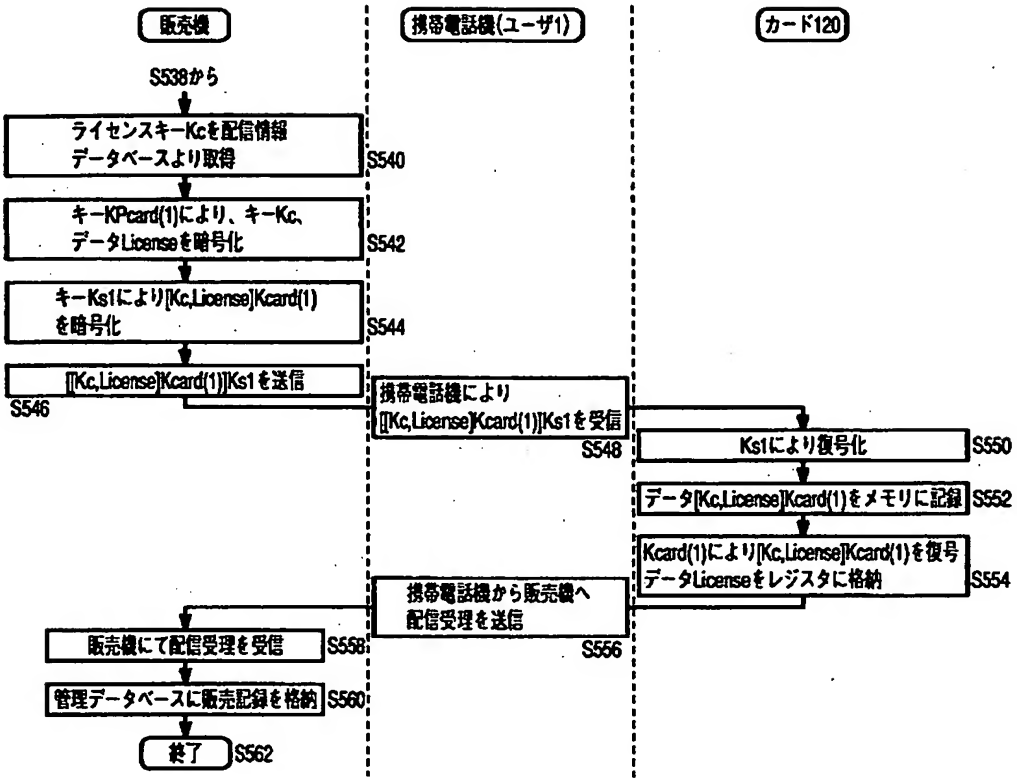
【図２７】


管理サーバ
2200
3000
配信情報データベース
304
送受信
360
2100
配信制御
暗号化
320
Ks発生
314
312
暗号化
復号
暗号化
BS1
322
318
316
ディスプレイ
キーボード
インターフェース
料金受理
2002
2012
2020
2004
2010

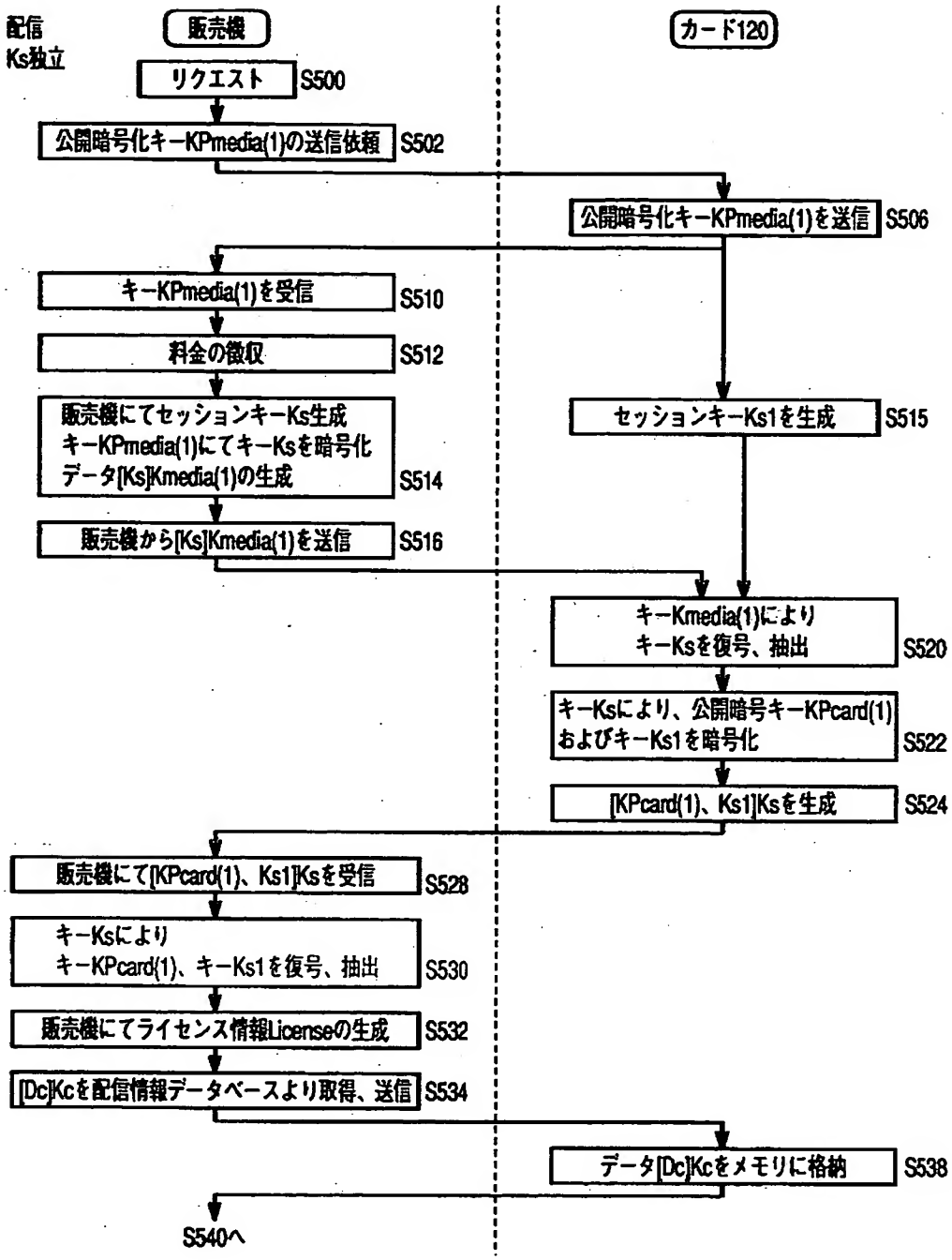
【図２８】


配信
Ks独立
販売機
携帯電話機(ユーザ1)
カード120
リクエスト S500
公開暗号化キーKPmedia(1)の送信依頼 S502
公開暗号化キーKPmedia(1)を送信 S506
携帯電話機から販売機へ
KPmedia(1)を送信
S508
キーKPmedia(1)を受信 S510
料金の徴収 S512
セッションキーKs1を生成 S515
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S514
販売機から[Ks]Kmedia(1)を送信
S516
携帯電話機1にて
[Ks]Kmedia(1)を受信
S518
キーKmedia(1)により
キーKsを復号、抽出
S520
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化
S522
[KPcard(1)、Ks1]Ksを生成
S524
携帯電話機から販売機へ
[KPcard(1)、Ks1]Ksを送信
S526
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出
S530
販売機にてライセンス情報Licenseの生成 S532
[Dc]Kcを配信情報データベースより取得、送信
S534
携帯電話機にて
データ[Dc]Kcを受信
S536
データ[Dc]Kcをメモリに格納 S538
S540へ

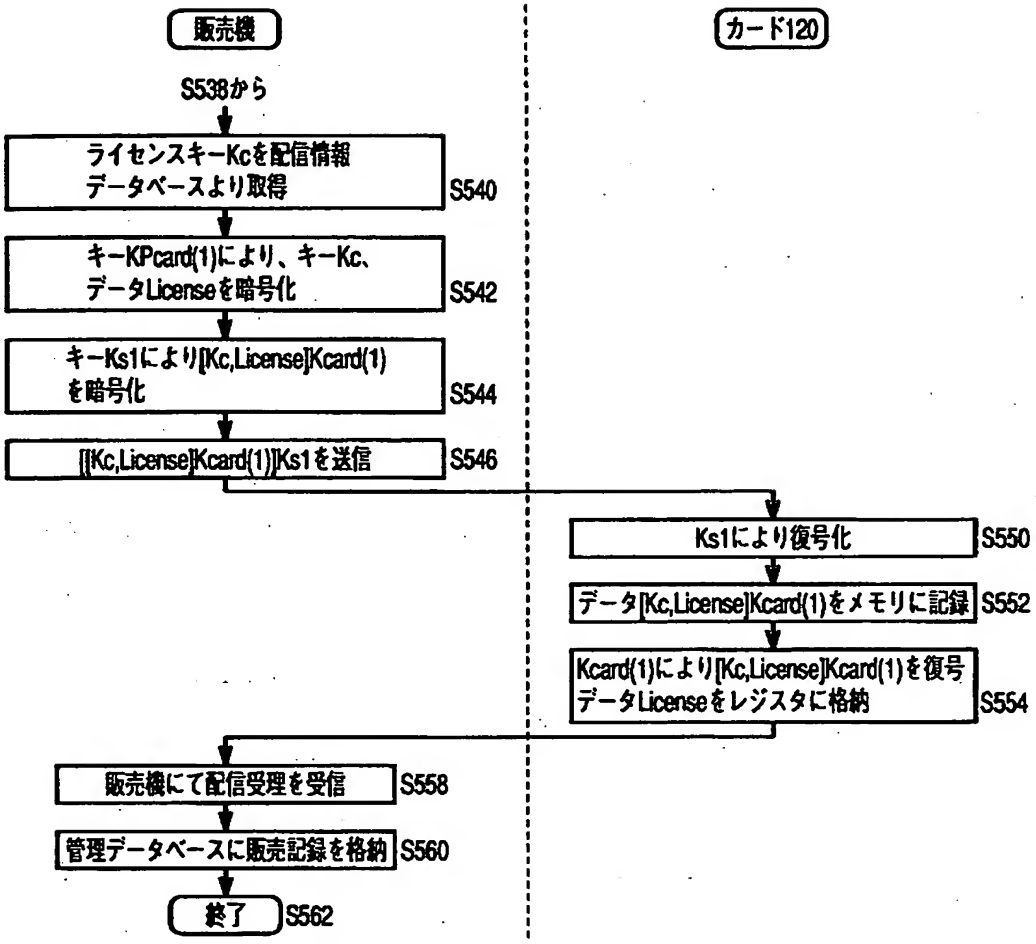
【図２９】


販売機
携帯電話機(ユーザ1)
カード120
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S548
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S554
携帯電話機から販売機へ配信受理を送信
S556
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

【図３０】


配信
Ks独立
販売機
カード120
リクエスト S500
公開暗号化キーKPmedia(1)の送信依頼 S502
公開暗号化キーKPmedia(1)を送信 S506
キーKPmedia(1)を受信 S510
料金の徴収 S512
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S514
セッションキーKs1を生成 S515
販売機から[Ks]Kmedia(1)を送信 S516
キーKmedia(1)により
キーKsを復号、抽出 S520
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S522
[KPcard(1)、Ks1]Ksを生成 S524
販売機にて[KPcard(1)、Ks1]Ksを受信 S528
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S530
販売機にてライセンス情報Licenseの生成 S532
[Dc]Kcを配信情報データベースより取得、送信 S534
データ[Dc]Kcをメモリに格納 S538
S540へ

【図３１】


販売機
カード120
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S554
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

【書類名】　要約書

【要約】

【課題】　著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供する。

【解決手段】　メモリカード１１０は、サーバから携帯電話網を介してデータバスＢＳ３に与えられるデータから、復号処理をすることによりセッションキーＫｓを抽出する。暗号化処理部１４０６は、セッションキーＫｓに基づいて、メモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を暗号化してデータバスＢＳ３を介してサーバに与える。レジスタ１５００は、復号されたライセンスＩＤ、ユーザＩＤ等のデータをサーバから受けとって格納し、メモリ１４１２は、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納する。

【選択図】　図５

出証特２０００－３０８５３１８

認定・付加情報

特許出願の番号	平成１１年　特許願　第２４１７４７号
受付番号	５９９００８３２０３５
書類名	特許願
担当官	坏　政光　　８８４４
作成日	平成１１年　９月　２日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000005223
- 【住所又は居所】 神奈川県川崎市中原区上小田中４丁目１番１号
- 【氏名又は名称】 富士通株式会社

【特許出願人】
- 【識別番号】 000005108
- 【住所又は居所】 東京都千代田区神田駿河台四丁目６番地
- 【氏名又は名称】 株式会社日立製作所

【特許出願人】
- 【識別番号】 000004167
- 【住所又は居所】 東京都港区赤坂４丁目１４番１４号
- 【氏名又は名称】 日本コロムビア株式会社

【特許出願人】
- 【識別番号】 000001889
- 【住所又は居所】 大阪府守口市京阪本通２丁目５番５号
- 【氏名又は名称】 三洋電機株式会社

【代理人】 申請人
- 【識別番号】 100064746
- 【住所又は居所】 大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 深見　久郎

【選任した代理人】
- 【識別番号】 100085132
- 【住所又は居所】 大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 森田　俊雄

【選任した代理人】
- 【識別番号】 100091409

次頁有

認定・付加情報（続き）

【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　伊藤　英彦
【選任した代理人】
【識別番号】　100096781
【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　堀井　豊

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００５２２３〕

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出 願 人 履 歴 情 報

識別番号　〔０００００４１６７〕

１．変更年月日　１９９０年　８月２１日
［変更理由］　新規登録
住　所　東京都港区赤坂４丁目１４番１４号
氏　名　日本コロムビア株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００１８８９〕

１．変更年月日　１９９３年１０月２０日
［変更理由］　住所変更
住　所　大阪府守口市京阪本通２丁目５番５号
氏　名　三洋電機株式会社